

QUANTIZATION CAUSES WAVES: SMOOTH FINITELY COMPUTABLE FUNCTIONS ARE AFFINE

VLADIMIR ANASHIN

ABSTRACT. Given an automaton (a letter-to-letter transducer) \mathfrak{A} whose input and output alphabets are $\mathbb{F}_p = \{0, 1, \dots, p-1\}$, one visualizes word transformations performed by \mathfrak{A} by a point set $\mathbf{P}(\mathfrak{A})$ of real plane \mathbb{R}^2 as follows: To an m -letter non-empty word $v = \gamma_{m-1}\gamma_{m-2}\dots\gamma_0$ over the alphabet \mathcal{A} put into the correspondence a rational number $0.v$ whose base- p expansion is $0.\gamma_{m-1}\gamma_{m-2}\dots\gamma_0$; then to every m -letter input word $w = \alpha_{m-1}\alpha_{m-2}\dots\alpha_0$ of the automaton \mathfrak{A} and to the respective m -letter output word $\mathfrak{a}(w) = \beta_{m-1}\beta_{m-2}\dots\beta_0$ (rightmost letters are feeded to/outputted from the automaton prior to leftmost ones) there corresponds a point $(0.w; 0.\mathfrak{a}(w))$ of the real unit square $[0, 1]^2$; denote $\mathbf{P}(\mathfrak{A})$ a closure (in the topology of \mathbb{R}^2) of the point set $(0.w; 0.\mathfrak{a}(w))$ where w ranges over the set \mathcal{W} of all non-empty words over the alphabet \mathbb{F}_p .

For a finite-state automaton \mathfrak{A} , it is shown that once some points of $\mathbf{P}(\mathfrak{A})$ constitute a smooth (of a class C^2) curve in \mathbb{R}^2 , the curve is a segment of a straight line with a rational slope; and there are only finitely many straight lines whose segments are in $\mathbf{P}(\mathfrak{A})$. Moreover, when identifying $\mathbf{P}(\mathfrak{A})$ with a subset of a 2-dimensional torus $\mathbb{T}^2 \subset \mathbb{R}^3$ (under a natural mapping of the real unit square $[0, 1]^2$ onto \mathbb{T}^2) the smooth curves from $\mathbf{P}(\mathfrak{A})$ constitute a collection of torus windings. In cylindrical coordinates either of the windings can be ascribed to a complex-valued function $\psi(x) = e^{i(Ax - 2\pi B(t))}$ ($x \in \mathbb{R}$) for suitable rational $A, B(t)$. Since $\psi(x)$ is a standard expression for a matter wave in quantum theory (where $B(t) = tB(t_0)$), and since transducers can be regarded as a mathematical formalization for causal discrete systems, the main result of the paper might serve as a mathematical reasoning why wave phenomena are inherent in quantum systems: This is because of causality principle and the discreteness of matter.

1. INTRODUCTION

In the paper, we examine C^2 -smooth real functions which can be computed (in some new but natural meaning which is rigorously defined below) on finite automata, i.e., on sequential machines that have only finite number of states. We show that all these functions are affine and, moreover, that they can be expressed as complex functions $e^{i(Ax+B)}$ and thus can be ascribed (also in some natural rigorous meaning) to matter waves from quantum theory.

A general problem of evaluation of real functions on abstract discrete machines naturally arose at the very moment the first digital computers had been invented. There are a number of various mathematical statements of the problem which depend both on specific mathematical model of a digital computer (the abstract machine) and on the representation of reals in some ‘digital’ form. For instance, real number computations on Turing machines constitute a core of theory of constructive reals and computable functions. The theory demonstrates intensive development for during more than half a century, see e.g. [36] and references therein. Sequential machines (also known as Mealy automata, or as finite-state letter-to-letter transducers) are, speaking loosely, Turing machines whose heads move only

in one direction. Sequential machines are therefore less power computers compared to general Turing machines; however, a number of real world phenomena and processes can be modelled by sequential machines since the latter can be considered as (non-autonomous) discrete dynamical systems. That is why the theory of functions computable by sequential machines, which constitutes a substantial part of automata theory, has numerous applications not only in mathematics itself (e.g., in real analysis, p -adic analysis, number theory, complexity theory, dynamics, etc.) but also in computer science, physics, linguistics and in many other sciences, see e.g. monographs [2, 3, 8, 9, 15, 29, 47] for details and references.

The paper was motivated by empirical data obtained during a research project related to an applied problem which assumed intensive computer experiments with automata modelling of various cryptographic primitives used in stream ciphers, hash functions, etc. Word transformations performed by the automata were visualised, namely, represented by points of the unit square $\mathbb{I}^2 = [0, 1] \times [0, 1]$ in real plane \mathbb{R}^2 so that coordinates of the points relate numerical (radix) representations of input words to the numerical representations of corresponding output words. It was noticed that once the modelled system was finite-state, and once input words were taken sufficiently long, some linear structures (looking like segments of straight lines and somewhat resembling pictures from a double-slit experiment in quantum physics, cf. Figures 1–2 and Figure 14) may appear in the graph, but more complicated structures like smooth curves of higher order had never been observed. A particular aim of the paper is to give mathematical explanation of the phenomenon and to characterize these linear structures.

But during the research it became evident that the problem (which actually is a question what smooth real functions can be modelled on finite automata) has applications not only to cryptography (see e.g. [3, Chapter 11]) but also may be related to mathematical formalism of quantum theory. As a matter of fact, the latter relation (which we believe does exist) can be regarded as a yet another answer to the following question discussed by A. Khrennikov in a series of papers devoted to so-called Prequantum Classical Statistical Field theory, see e.g. [23, 22]: *Why mathematical formalism of quantum theory (which is based on the theory of linear operators on Hilbert spaces) is essentially linear although a number of quantum phenomena demonstrate an extremely non-linear behavior?*

Thus the goal of the paper is twofold:

- firstly, to characterize real functions which can be computed by finite automata; and
- secondly, to give (using obtained description of the functions) some mathematical reasoning why wave phenomena are inherent in quantum systems.

The major part of the paper focuses on real functions which can be computed by finite automata while the said mathematical reasoning is considered in a closing section which contains a discussion of possible applications of mathematical results of the paper to quantum theory. We are not going to discuss cryptographic applications here; they will be postponed to forthcoming papers.

In the paper, by a general automaton (whose set of states is not necessarily finite) we mean a machine which performs letter-by-letter transformations of words over input alphabet into words over output alphabet: Once a letter is feeded to the automaton, the automaton updates its current state (which initially is fixed and so is the same for all input words) to the next one and produces corresponding output letter. Both the next state and the output letter depend both on the current state and on the input letter. Therefore each letter of output word depends *only* on those letters of input word which have already been feeded to the automaton. An input word is a finite sequence of letters; the letters can naturally be ascribed

to ‘causes’ while letters of the corresponding output word can be regarded as ‘effects’. ‘Causality’ just means that effects depend only on causes that ‘already have happened’; therefore an automaton is an adequate mathematical formalism for a specific manifestation of causality principle once we assume that there exist only finitely many causes and effects, cf., e.g., [44, 45].

When studying real functions that can be computed by an automaton \mathfrak{A} whose input/output alphabets are $\mathcal{A} = \{0, 1, \dots, p-1\}$ (where $p > 1$ is an integer from $\mathbb{N} = \{1, 2, 3, \dots\}$) most authors follow common approach which described in e.g. [15, Chapter XIII, Section 4]: They associate an infinite word $\alpha_1\alpha_2\dots\alpha_n\dots$ over \mathcal{A} to a real number whose base- p expansion is $0.\alpha_1\alpha_2\dots\alpha_n\dots = \sum_{i=1}^{\infty} \alpha_i p^{-i}$ and consider a real function $d_{\mathfrak{A}}$ defined as follows: Given $x \in [0, 1]$, take its base- p expansion $x = \sum_{i=1}^{\infty} \alpha_i p^{-i}$; then produce an infinite output sequence $\beta_1\beta_2\dots\beta_n\dots$ of \mathfrak{A} by successfully feeding the automaton with the letters α_1, α_2 , etc., and put $d_{\mathfrak{A}}(x) = \sum_{i=1}^{\infty} \beta_i p^{-i}$. Being fed by infinite input sequence $\alpha_1\alpha_2\dots\alpha_n\dots$, the automaton \mathfrak{A} produces a unique infinite output sequence $\beta_1\beta_2\dots\beta_n\dots$; therefore the function $d_{\mathfrak{A}}$ is well defined everywhere on the real closed unit interval (segment) $\mathbb{I} = [0, 1]$ with the exception of maybe a countable set $D \subset [0, 1]$ of points; namely, of those having two distinct base- p expansions $0.\gamma_1\gamma_2\dots\gamma_n0\dots0\dots = 0.\gamma_1\gamma_2\dots\gamma_{n-1}(\gamma_n - 1)(p-1)\dots(p-1)\dots$. The point set $\mathbf{M}(\mathfrak{A}) = \{(x; d_{\mathfrak{A}}(x)) \in \mathbb{R}^2: x \in [0, 1]\}$ can be considered as a graph of the real function $d_{\mathfrak{A}}$ specified by the automaton \mathfrak{A} (every time, before being fed by the very first letter of each infinite input word the automaton \mathfrak{A} is assumed to be in a fixed state s_0 , the *initial state*). Indeed, $d_{\mathfrak{A}}(x)$ is defined uniquely for $x \in [0, 1] \setminus D$ and $d_{\mathfrak{A}}(x)$ can be ascribed to at most two values for $x \in D$; so $d_{\mathfrak{A}}$ can be treated a real function which is defined on the unit segment $[0, 1]$ and has not more that a countable number points of discontinuity in $[0, 1]$. In the sequel we refer $\mathbf{M}(\mathfrak{A})$ as to the *Monna graph* of the automaton \mathfrak{A} , cf. Subsection 2.5.

The said common approach (and its various generalisations) is utilised in numerous papers, see e.g. [10, 11, 27, 28, 39]. Speaking loosely, the common approach looks as if one feeds the automaton \mathfrak{A} by a base- p expansion of a real number $x \in [0, 1]$ so that *leftmost* (i.e., the most significant) *digits are feeded to the automaton prior to rightmost ones* and observes output as real numbers since the automaton outputs accordingly leftmost digits of the base- p expansion of $d_{\mathfrak{A}}(x) \in [0, 1]$ prior to rightmost ones thus ascribing to the automaton \mathfrak{A} the real function $d_{\mathfrak{A}}$. We stress that the function $d_{\mathfrak{A}}$ is well defined almost everywhere on $[0, 1]$ due to *namely that order* in which digits of base- p expansion are feeded to (and outputted from) the automaton \mathfrak{A} .

A crucial difference of the approach used in our paper from the mentioned one is that *the order we feed digits to (and read digits from) the automaton is inverse*: Namely,

- (i) given a real number $x \in [0, 1]$, we represent x via base- p expansion $x = 0.\alpha_1\alpha_2\dots\alpha_n\dots$ (we take both expansions if x has two distinct ones);
- (ii) from the base- p expansion $0.\alpha_1\alpha_2\dots\alpha_n\dots$ we derive corresponding sequence $\alpha_1, \alpha_1\alpha_2, \alpha_1\alpha_2\alpha_3, \dots$ of words; then
- (iii) feeding the automaton \mathfrak{A} successively by the words $\alpha_1, \alpha_1\alpha_2, \alpha_1\alpha_2\alpha_3, \dots$ so that *rightmost letters are feeded to \mathfrak{A} prior to leftmost ones* we obtain corresponding output word sequence $\zeta_{11}, \zeta_{12}\zeta_{22}, \zeta_{13}\zeta_{23}\zeta_{33}, \dots$;
- (iv) to the output sequence we put into a correspondence the sequence $\mathcal{S}(x)$ of rational numbers whose base- p expansions are $0.\zeta_{11}, 0.\zeta_{12}\zeta_{22}, 0.\zeta_{13}\zeta_{23}\zeta_{33}, \dots$ thus obtaining a point set $\mathcal{X}(x) = \{(0.\alpha_1\dots\alpha_i; 0.\zeta_{1i}\zeta_{2i}\dots\zeta_{ii}): i = 1, 2, \dots\}$ in the real unit square $\mathbb{I}^2 = [0, 1] \times [0, 1]$; after that
- (v) we consider the set $\mathcal{F}(x)$ of *all* cluster points of the sequence $\mathcal{S}(x)$;

- (vi) finally, we specify a *real plot* (or, briefly, a plot) of the automaton \mathfrak{A} as a union $\mathbf{P}(\mathfrak{A}) = \cup_{x \in [0,1], y \in \mathcal{F}(x)} ((x; y) \cup \mathcal{X}(x))$.

In other words, $\mathbf{P}(\mathfrak{A})$ is a closure in the unit square \mathbb{I}^2 of the union $\cup_{i=1}^{\infty} \mathbf{L}_i(\mathfrak{A})$ where $\mathbf{L}_i(\mathfrak{A}) = \{(0.\alpha_1 \dots \alpha_i; 0.\zeta_{1i} \zeta_{2i} \dots \zeta_{ii}) : x \in \mathbb{I}\}$ is the *i-th layer* of the plot $\mathbf{P}(\mathfrak{A})$. That is, the plot $\mathbf{P}(\mathfrak{A})$ can be considered as a ‘limit’ of the sequence of sets $\cup_{i=1}^n \mathbf{L}_i(\mathfrak{A})$, the *approximate plots* at word length N , while $N \rightarrow \infty$ (see more formal definitions in Subsection 2.5). Note that according to automata 0-1 law (cf. [3, Proposition 11.15] and [6]) the plot $\mathbf{P}(\mathfrak{A})$ of arbitrary automaton \mathfrak{A} can be of two kinds only: Either $\mathbf{P}(\mathfrak{A}) = \mathbb{I}^2$ or $\mathbf{P}(\mathfrak{A})$ is a (Lebesgue) measure-0 closed subset of \mathbb{R}^2 . Moreover, if the number of states of the automaton \mathfrak{A} is finite (further in the paper these automata are referred to as *finite* ones), then the second case takes place.

We stress crucial advantage of real plots over Monna graphs: In a contrast to the Monna graph $\mathbf{M}(\mathfrak{A})$, a real plot $\mathbf{P}(\mathfrak{A})$ is capable of showing true long-term behavior of automaton \mathfrak{A} (i.e., when \mathfrak{A} is feeded by sufficiently long words) rather than a short-term behaviour displayed by the Monna graph $\mathbf{M}(\mathfrak{A})$ since due to the very construction of the real plot the higher order (i.e., the most significant) digits of the real number represented by the output word are formed by the latest outputted letters of the output word whereas the construction of the Monna graph assumes that the higher order digits are formed by the earliest outputted letters. This results in a drastically different appearances of the real plot and of the Monna graph: Real plot clearly demonstrates that corresponding automaton is ‘ultimately linear’ (that is, exhibits linear long-term behavior), cf. Figures 1–3; whereas the Monna graph is incapable to reveal this important feature of the automaton, cf. Figure 4. This is the main reason why in the paper we focus on real plots of automata rather than on their Monna graphs.

Therefore when specifying a notion of computability of a real-valued function $g: G \rightarrow [0, 1]$ (where $G \subset [0, 1]$) on automata, at least two different approaches do exist: The first one is to speak of the case when the graph $\mathbf{G}(g) = \{(x; g(x)) : x \in G\}$ of the function G lie completely in $\mathbf{M}(\mathfrak{A})$ for some automaton \mathfrak{A} while the second one is to consider the case when $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$. Papers [10, 11, 27, 28, 39] mentioned above basically deal with the computability in the first meaning whereas our’s paper deals with the computability of the second kind. Note that classes of real functions which are computable on finite automata are different depending on the meaning: For instance, the function $[px]$ (where $[a]$ stands for the integral part of $a \in \mathbb{R}$, i.e., for the biggest integer not exceeding a) is not computable in the first meaning but is computable in the second one whilst the function $p^{-1}x$ is computable in the first meaning but is not computable in the second one.

To the best of our knowledge, our approach (which is based on real plots rather than on Monna graphs) was originally used in [3] and was never considered before by other authors.

In the sequel we refer real functions $g: G \rightarrow [0, 1]$ with domain $G \subset [0, 1]$ as to *finitely computable* if there exists a finite automaton \mathfrak{A} whose real plot contains the graph of the function g ; i.e., if $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$. Main result of our paper is Theorem 5.1 which characterizes all finitely computable C^2 -functions g defined on a sub-segment $D = [a, b] \subset [0, 1]$: The theorem yields that *if a finitely computable function $g: D \rightarrow [0, 1]$ is twice differentiable and if its second derivative is continuous everywhere on D then g is necessarily affine of the form $g(x) = Ax + B$ for suitable rational p -adic A, B (that is, for A, B which can be represented by irreducible fractions whose denominators are co-prime to p). Moreover, this is true in n -dimensional case as well (Theorem 5.5).*

FIGURE 1. Approximate plot of an automaton at word length 16

FIGURE 2. Approximate plot of the same automaton at word length 17

FIGURE 3. Cluster points of the plot of the same automaton

FIGURE 4. The Monna graph of the same automaton

In view of Theorem 5.1 it is noteworthy that despite the classes of functions computable on finite automata are different depending on the meaning the computability is understood, nonetheless if a function $g: [0, 1] \rightarrow [0, 1]$ is everywhere differentiable on $(0, 1)$ and $\mathbf{G}(g) \subset \mathbf{M}(\mathfrak{A})$ for some finite automaton \mathfrak{A} with binary input/output alphabets then g is necessarily affine, see [28]. In [27] it is shown that a similar assertion holds for multivariate continuously differentiable functions and arbitrary finite alphabets. Therefore finite automata should be judged as rather ‘weak computers’ in all meanings since only quite simple real functions can be evaluated on these devices. From this view, results of the current paper are some contribution to the theory of computable real functions.

It is worth mentioning right now that actually our proof reveals a basic reason why smooth functions which can be represented by finite automata are necessarily affine: This is because *squaring can not be performed by a finite automaton*; that is, an automaton which, being fed by a base- p expansion of n , outputs a base- p expansion of n^2 for every positive integer n , can not be finite (the latter is a well-known fact from automata theory, see e.g., [8, Theorem 2.2.3]).

It is also worth mentioning that the question when $\mathbf{G}(g) \subset \mathbf{M}(\mathfrak{A})$ is somewhat easier to handle than the question when $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$. Indeed, in the first case once the automaton \mathfrak{A} is feeded by an infinite word $\dots \alpha_3 \alpha_2 \alpha_1$, the word is treated as a base- p expansion of a unique real number $x = 0.\alpha_1 \alpha_2 \alpha_3 \dots \in [0, 1]$, corresponding output of \mathfrak{A} is also an infinite word $\dots \beta_3 \beta_2 \beta_1$ which also is treated as a base- p expansion of a unique real number $y = 0.\beta_1 \beta_2 \beta_3 \dots \in [0, 1]$. This results in a unique point $(x; y)$ of the unit square \mathbb{I}^2 in the first case; whilst in the second case the automaton \mathfrak{A} , being feeded by the infinite word $\dots \alpha_3 \alpha_2 \alpha_1$, produces generally an infinite point set of a cardinality continuum: The set is a closure of the point set $\{(0.\alpha_n \alpha_{n-1} \dots \alpha_1; 0.\beta_n \beta_{n-1} \dots \beta_1) : n = 1, 2, \dots\}$ in \mathbb{I}^2 . Due to this reason during the proofs we have to use more complicated techniques from real analysis which in some cases we combine with methods of p -adic analysis. Therefore some proofs are involved; but to make general idea of a proof as transparent as possible in the sequel we explain it in loose terms when appropriate.

Last but not least: Our approach reveals another important feature of smooth functions which can be computed on finite automata. From Figure 3 it can be clearly observed that limit points of the plot constitute a torus winding if one converts a unit square into torus by gluing together opposite sides of the square. This is not occasional: Our Theorem 5.1 yields that *if the unit square \mathbb{I}^2 is mapped onto a torus $\mathbb{T}^2 \subset \mathbb{R}^3$, the smooth curves from the plot become torus windings*; and these windings after being represented in cylindrical coordinates are described by complex-valued functions $e^{i(Ax+B)}$ ($x \in [0, 1]$), see Corollary 3.13. But in quantum theory the latter exponential functions are ascribed to matter waves (cf., de Broglie waves); therefore, since automata can be considered as models for discrete casual systems, the results of our paper give some mathematical evidence that matter waves are inherent in quantum systems merely due to causality principle and discreteness of matter (quantization). We discuss these possible connections to physics in Section 6.

Note that for not to overload the paper with extra calculations we consider only automata whose input and output alphabets consist of p letters $0, 1, \dots, p-1$ where $p > 1$ is a prime number though our approach can be expanded to the case when p is arbitrary integer greater than 1 (and even to the case when p is not necessarily an integer, see Section 6). For a prime p , we naturally associate when necessary letters of the alphabet $0, 1, \dots, p-1$ to residues modulo p , i.e., to elements of a finite field \mathbb{F}_p .

The paper is organized as follows:

- In Section 2 we recall basic definitions as well as some (mostly known) facts from combinatorics of words, from automata theory, from p -adic analysis, and from knot theory. Also in this section we formally introduce the notion of real plot of automaton and examine its basic properties.
- In Section 3 we completely describe cluster points of real plots of finite autonomous automata and of finite affine automata: We show that the points constitute links of torus knots.
- In Section 4 we prove numerous (mostly technical) results on finitely computable functions; that is, on real functions whose graphs lie in plots of finite automata. Loosely speaking, in the section we (rigorously) develop techniques to examine real functions computed on finite automata as if the automata are feeded by base- p expansions of real arguments of the functions so that less significant digits are feeded to automaton prior to more significant ones.
- Section 5 contains main results of the paper: We prove that once a finitely computable function is C^2 -smooth than it is affine and may be associated

to a finite collection of complex-valued functions $\Psi(x, \ell) = e^{i(Ax - 2\pi p^\ell B)}$, ($x \in \mathbb{R}; \ell \in \mathbb{N}_0$) for suitable rational numbers A, B which are p -adic integers. We prove a multivariate version of the theorem as well.

- In Section 6 we discuss possible connections of the main results to informational interpretation of quantum theory. We argue that the results show that wave function is a mathematical consequence of two basic assumptions which are causality principle and discreteness of matter: We show that using β -expansions of real numbers (where $\beta = 1 + \tau$ and $\tau > 0$ is small) rather than base- p expansions for positive integer $p > 1$, main results of the paper imply that a quantum system may be considered as a finite automaton which calculates functions $e^{i(Ax - 2\pi \beta^\ell B)}$; but the functions are approximately equal to $a \cdot e^{i(Ax - 2\pi t B)}$ when $t = \ell\tau$ since τ is small and thus $(1 + \tau)^\ell \approx 1 + \ell\tau$; moreover, $\beta = 1 + \tau$ implies that both input and output alphabets of the automaton must be necessarily binary, i.e., $\{0, 1\}$. Therefore one may say that the automaton produces waves $a \cdot e^{i(Ax - 2\pi t B)}$ (since variables $x, t \in \mathbb{R}$ may be regarded as ‘position’ and ‘time’ respectively) from bits. This may serve a mathematical evidence in favour of J. A. Wheeler’s *It from bit* doctrine which suggests that all things physical (‘its’) are information-theoretic in origin (‘from bits’), [46].

2. PRELIMINARIES

Technically the paper is a sort of interplay between real analysis and p -adic analysis; but although real analysis is the tool we mostly use in proofs, in some important places we also use p -adic analysis to examine specific properties of automata maps since the maps actually are 1-Lipschitz functions w.r.t. p -adic metric. This is why we first recall some facts about words over a finite alphabet, p -adic integers, and automata.

2.1. Few words about words. An *alphabet* is just a finite non-empty set \mathcal{A} ; further in the paper usually $\mathcal{A} = \{0, 1, \dots, p-1\} = \mathbb{F}_p$. Elements of \mathcal{A} elements are called *symbols*, or *letters*. By the definition, a *word of length n over alphabet \mathcal{A}* is a finite sequence (stretching from right to left) $\alpha_{n-1} \cdots \alpha_1 \alpha_0$, where $\alpha_{n-1}, \dots, \alpha_1, \alpha_0 \in \mathcal{A}$. The number n is called the *length* of the word $w = \alpha_{n-1} \cdots \alpha_1 \alpha_0$ and is denoted via $\Lambda(w)$. The *empty word* ϕ is a sequence of length 0, that is, the one that contains no symbols. Given a word $w = \alpha_{n-1} \cdots \alpha_1 \alpha_0$, any word $v = \alpha_{k-1} \cdots \alpha_1 \alpha_0$, $k \leq n$, is called a *prefix* of the word w ; whereas any word $u = \alpha_{n-1} \cdots \alpha_{i+1} \alpha_i$, $0 \leq i \leq n-1$ is called a *suffix* of the word w . Every word $\alpha_j \cdots \alpha_{i+1} \alpha_i$ where $n-1 \geq j \geq i \geq 0$ is called a *subword* of the word $w = \alpha_{n-1} \cdots \alpha_1 \alpha_0$. Given words $a = \alpha_{n-1} \cdots \alpha_1 \alpha_0$ and $b = \beta_{k-1} \cdots \beta_1 \beta_0$, the *concatenation* ab is the following word (of length $n+k$):

$$ab = \alpha_{n-1} \cdots \alpha_1 \alpha_0 \beta_{k-1} \cdots \beta_1 \beta_0.$$

Given a word w , its k -times concatenation is denoted via $(w)^k$:

$$(w)^k = \underbrace{ww \dots w}_{k \text{ times}}.$$

We denote via \mathcal{W} the set of all non-empty words over $\mathcal{A} = \{0, 1, \dots, p-1\}$ and via \mathcal{W}_ϕ the set of all words including the empty word ϕ . In the sequel the set of all n -letter words over the alphabet \mathbb{F}_p we denote as \mathcal{W}_n ; so $\mathcal{W} = \bigcup_{n=1}^{\infty} \mathcal{W}_n$. To every word $w = \alpha_{n-1} \cdots \alpha_1 \alpha_0$ we put into the correspondence a non-negative integer $\text{num}(w) = \alpha_0 + \alpha_1 \cdot p + \dots + \alpha_{n-1} \cdot p^{n-1}$. Thus num maps the set \mathcal{W} of all non-empty finite words over the alphabet \mathcal{A} onto the set $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ of all non-negative integers. We will also consider a map ρ of the set \mathcal{W} into the real unit

half-open interval $[0, 1)$; the map ρ is defined as follows: Given $w = \beta_{r-1} \dots \beta_0 \in \mathcal{W}$, put

$$\rho(w) = \text{num}(w) \cdot p^{-\Lambda(w)} = \frac{\beta_0 + \beta_1 p + \dots + \beta_{r-1} p^{r-1}}{p^r} = 0.\beta_{r-1} \dots \beta_0 \in [0, 1). \quad (2.1)$$

We also use the notation $0.w$ for $0.\beta_{r-1} \dots \beta_0$.

Along with finite words we also consider (left-)infinite words over the alphabet \mathcal{A} ; the ones are the infinite sequences of the form $\dots \alpha_2 \alpha_1 \alpha_0$ where $\alpha_i \in \mathcal{A}$, $i \in \mathbb{N}_0$. For infinite words the notion of a prefix and of a subword are defined in the same way as for finite words; whilst suffix is not defined. Let an infinite word w be eventually periodic, that is, let $w = \dots \beta_{t-1} \beta_{t-2} \dots \beta_0 \beta_{t-1} \beta_{t-2} \dots \beta_0 \alpha_{r-1} \alpha_{r-2} \dots \alpha_0$ for $\alpha_i \beta_j \in \mathcal{A}$; then the subword $\beta_{t-1} \beta_{t-2} \dots \beta_0$ is called a *period* of the word w and the suffix $\alpha_{r-2} \dots \alpha_0$ is called the pre-period of the word w . Note that a pre-period may be an empty word while a period can not. We write the eventually periodic word w as $w = (\beta_{t-1} \beta_{t-2} \dots \beta_0)^\infty \alpha_{r-1} \alpha_{r-2} \dots \alpha_0$.

2.2. p -adic numbers. See [17, 20, 26] for introduction to p -adic analysis or comprehensive monographs [31, 38] for further reading.

Fix a prime number p and denote respectively via $\mathbb{N} = \{1, 2, \dots\}$ and $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ the set of all positive rational integers and the ring of all rational integers. Given $n \in \mathbb{N} = \mathbb{N}_0 \setminus \{0\}$, the p -adic absolute value of n is $|n|_p = p^{-\text{ord}_p n}$, where $p^{\text{ord}_p n}$ is the largest power of p which is a factor of n ; so $n = n' \cdot p^{\text{ord}_p n}$ where $n' \in \mathbb{N}$ is co-prime to p . By putting $|0|_p = 0$, $|-n|_p = |n|_p$ and $|n/m|_p = |n|_p / |m|_p$ for $n, m \in \mathbb{Z}$, $m \neq 0$ we expand the p -adic absolute value to the whole field \mathbb{Q} of rational numbers. Given an absolute value $|\cdot|_p$, we define a metric in a standard way: $|a-b|_p$ is a p -adic metric on \mathbb{Q} . The field \mathbb{Q}_p of p -adic numbers is a completion of the field \mathbb{Q} of rational numbers w.r.t. the p -adic metric while the ring \mathbb{Z}_p of p -adic integers is a ring of integers of \mathbb{Q}_p ; and the ring \mathbb{Z}_p is a completion of \mathbb{Z} w.r.t. the p -adic metric. The ring \mathbb{Z}_p is compact w.r.t. the p -adic metric: Actually \mathbb{Z}_p is a ball of radius 1 centered at 0; namely $\mathbb{Z}_p = \{r \in \mathbb{Q}_p : |r|_p \leq 1\}$. Balls in \mathbb{Q}_p are *clopen*; that is, both closed and open w.r.t. the p -adic metric.

A p -adic number $r \in \mathbb{Q}_p \setminus \{0\}$ admits a unique p -adic canonical expansion $r = \sum_{i=k}^{\infty} \alpha_i p^i$ where $\alpha_i \in \{0, 1, \dots, p-1\}$, $k \in \mathbb{Z}$, $\alpha_k \neq 0$. Note that then any p -adic integer $z \in \mathbb{Z}_p$ admits a unique representation $z = \sum_{i=0}^{\infty} \alpha_i p^i$ for suitable $\alpha_i \in \{0, 1, \dots, p-1\}$. The latter representation is called a *canonical form* (or, a *canonical representation*) of the p -adic integer $z \in \mathbb{Z}_p$; the i -th coefficient α_i of the expansion will be referred to as the i -th p -adic digit of z and denoted via $\alpha_i = \delta_i(z)$. It is clear that once $z \in \mathbb{N}_0$, the i -th p -adic digit $\delta_i(z)$ of z is just the i -th digit in the base- p expansion of z . Note also that a p -adic integer $z \in \mathbb{Z}_p$ is a *unity* of \mathbb{Z}_p (i.e., has a multiplicative inverse $z^{-1} \in \mathbb{Z}_p$) if and only if $\delta_0(z) \neq 0$; so any p -adic number $z \in \mathbb{Q}_p$ has a unique representation of the form $z = z' \cdot |z|_p^{-1}$ where $z' \in \mathbb{Z}_p$ is a unity.

The p -adic integers may be associated to infinite words over the alphabet $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ as follows: Given a p -adic integer $z \in \mathbb{Z}_p$, consider its canonical expansion $z = \sum_{i=0}^{\infty} \alpha_i \cdot p^i$; then denote via $\text{wrd}(z)$ the infinite word $\dots \alpha_2 \alpha_1 \alpha_0$ (allowing some freedom of saying we will sometimes refer $\text{wrd}(z)$ as to a *base- p expansion of $z \in \mathbb{Z}_p$*). Vice versa, given a left-infinite word $w = \dots \alpha_2 \alpha_1 \alpha_0$ we denote via $\text{num}(w) = \sum_{i=0}^{\infty} \alpha_i \cdot p^i$ corresponding p -adic integer whose base- p expansion is w thus expanding the mapping num defined in Subsection 2.1 to the case of infinite words as well. It is worth noticing here that addition and multiplication of p -adic integers can be performed by using the same school-textbook algorithms for addition/multiplication of non-negative integers represented via their base- p expansions

with the only difference: The algorithms are applied to infinite words that correspond to p -adic canonical forms of summands/multipliers rather than to a finite words which are base- p expansions of summands/multipliers.

Given $n \in \mathbb{N}$ and a canonical expansion $z = \sum_{i=0}^{\infty} \alpha_i p^i$ for $z \in \mathbb{Z}_p$, denote $z \bmod p^n = \sum_{i=0}^{n-1} \alpha_i p^i$. The mapping $\bmod p^n: z \mapsto z \bmod p^n$ is a ring epimorphism of \mathbb{Z}_p onto the residue ring $\mathbb{Z}/p^n\mathbb{Z}$ (under a natural representation of elements of the residue ring by the least non-negative residues $\{0, 1, \dots, p^n - 1\}$).

The series in the right-hand side of the canonical form converges w.r.t. the p -adic metric; that is, the sequence of partial sums $z \bmod p^n$ converges to z w.r.t. the p -adic metric: $\lim_{n \rightarrow \infty} (z \bmod p^n) = z$. It is worth noticing here that arbitrary infinite series $\sum_{i=0}^{\infty} r_i$ where $r_i \in \mathbb{Q}_p$ converges in \mathbb{Q}_p (i.e., w.r.t. p -adic metric) if and only if $\lim_{i \rightarrow \infty} |r_i|_p = 0$ since p -adic metric is *non-Archimedean*; that is, it satisfies *strong triangle inequality* $|x - y|_p \leq \max\{|x - z|_p, |z - y|_p\}$ for all $x, y, z \in \mathbb{Q}_p$.

Note that $z \in \mathbb{N}_0$ if and only if all but a finite number of coefficients α_i in the canonical form are 0 while $z \in \{-1, -2, -3, \dots\}$ if and only if all but a finite number of α_i are $p - 1$. Further we will need a special representation for *p -adic integer rationals*; that is, for those rational numbers z which at the same time are p -adic integers, i.e., for $z \in \mathbb{Z}_p \cap \mathbb{Q}$. Note that $z \in \mathbb{Z}_p \cap \mathbb{Q}$ if and only if z can be represented by an irreducible fraction $z = a/b$, $a \in \mathbb{Z}, b \in \mathbb{N}$ where b is co-prime to p . The following proposition is well known, cf., e.g., [16, Theorem 10]:

Proposition 2.1. *A p -adic integer z is rational (i.e., $z \in \mathbb{Z}_p \cap \mathbb{Q}$) if and only if the sequence of coefficients of its canonical form is eventually periodic:*

$$z = \alpha_0 + \alpha_1 p + \dots + \alpha_{r-1} p^{r-1} + (\beta_0 + \beta_1 p + \dots + \beta_{t-1} p^{t-1}) p^r + (\beta_0 + \beta_1 p + \dots + \beta_{t-1} p^{t-1}) p^{r+t} + (\beta_0 + \beta_1 p + \dots + \beta_{t-1} p^{t-1}) p^{r+2t} + \dots \quad (2.2)$$

for suitable $\alpha_j, \beta_i \in \{0, 1, \dots, p-1\}$, $r \in \mathbb{N}_0$, $t \in \mathbb{N}$ (the sum $\alpha_0 + \alpha_1 p + \dots + \alpha_{r-1} p^{r-1}$ is absent in the above expression once $r = 0$).

In other words, once a p -adic integer z is represented in its canonical form, $z = \sum_{i=0}^{\infty} \gamma_i p^i$, the corresponding infinite word $\dots \gamma_1 \gamma_0$ is eventually periodic: $\dots \gamma_1 \gamma_0 = (\beta_{t-1} \dots \beta_0)^\infty \alpha_{r-1} \dots \alpha_0$. It is clear that given $z \in \mathbb{Z}_p \cap \mathbb{Q}$, both r and t are not unique: For instance,

$$(\beta_{t-1} \dots \beta_0)^\infty \alpha_{r-1} \dots \alpha_0 = (\beta_0 \beta_{t-1} \dots \beta_1 \beta_0 \beta_{t-1} \dots \beta_1)^\infty \alpha_r \alpha_{r-1} \dots \alpha_0,$$

where $\alpha_r = \beta_0$. But once both pre-periodic and periodic parts (the prefix $\alpha_{r-1} \dots \alpha_0$ and the word $\beta_{t-1} \dots \beta_0$) are taken the shortest possible, both the *pre-period length* r and the *period length* t are unique for a given p -adic rational integer $z \in \mathbb{Z}_p \cap \mathbb{Q}$; we refer to $\alpha_{r-1} \dots \alpha_0$ and to $\beta_{t-1} \beta_{t-2} \dots \beta_1 \beta_0$ as to *pre-period* of z and *period* of z accordingly.

Given $z \in \mathbb{Z}_p \cap \mathbb{Q}$ we mostly assume further that in the representation $z = \alpha_0 + \dots + \alpha_{r-1} p^{r-1} + (\beta_0 + \dots + \beta_{t-1} p^{t-1}) \cdot \sum_{j=0}^{\infty} p^{r+tj}$ (respectively, in eventually periodic infinite word $\text{wrđ}(z) = (\beta_{t-1} \dots \beta_0)^\infty \alpha_{r-1} \dots \alpha_0$ that corresponds to z) r is a pre-period length and t is a period length. Note that a pre-period may be an empty word (i.e., of length 0) while a period can not.

Rational p -adic integers can also be represented as fractions of a special kind:

Proposition 2.2. *A p -adic integer $z \in \mathbb{Z}_p$ is rational if and only if there exist $t \in \mathbb{N}$, $c \in \mathbb{Z}$, $d \in \{0, 1, \dots, p^t - 2\}$ such that*

$$z = c + \frac{d}{p^t - 1}. \quad (2.3)$$

Proof. Indeed, $z \in \mathbb{Z}_p \cap \mathbb{Q}$ if and only if z is of the form (2.2); therefore

$$z = (\alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1} p^{r-1} - p^r) + p^r \left(1 - \frac{\beta_0 + \beta_1 p + \cdots + \beta_{t-1} p^{t-1}}{p^t - 1} \right) =$$

$$(\alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1} p^{r-1} - p^r + q) + \frac{\zeta_0 + \zeta_1 p + \cdots + \zeta_{t-1} p^{t-1}}{p^t - 1} \quad (2.4)$$

where $\zeta_0 + \zeta_1 p + \cdots + \zeta_{t-1} p^{t-1}$ is a base- p expansion of the least non-negative residue s of $p^r(p^t - 1 - (\beta_0 + \beta_1 p + \cdots + \beta_{t-1} p^{t-1})) = (p^t - 1)q + s$ modulo $p^t - 1$. \square

Note 2.3. Recall that $(1 - p^m)^{-1} = \sum_{i=0}^{\infty} p^{mi} \in \mathbb{Z}_p$, for every $m \in \mathbb{N}$.

Note 2.4. Note that once in (2.4) r is a pre-period length and t is a period length of $z \in \mathbb{Z}_p \cap \mathbb{Q}$, the representation (2.3) is unique; that is, the choice of c and d in (2.3) is unique.

In the sequel we often use base- p expansions of p -adic rational integers reduced modulo 1 (recall that if $y \in \mathbb{R}$ then by the definition $y \bmod 1 = y - \lfloor y \rfloor \in [0, 1) \subset \mathbb{R}$) along with their p -adic canonical forms. For reader's convenience, we now summarize some facts on connections between these representations.

It is very well known that a base- p expansion of a rational number is eventually periodic; that is, given $x \in \mathbb{Q} \cap [0, 1]$, the base- p expansion for x is

$$x = 0.\chi_0 \dots \chi_{k-1}(\xi_0 \dots \xi_{n-1})^\infty =$$

$$\chi_0 p^{-1} + \chi_1 p^{-2} + \cdots + \chi_{k-1} p^{-k} + \xi_0 p^{-k-1} + \xi_1 p^{-k-2} + \cdots + \xi_{n-1} p^{-k-n} +$$

$$\xi_0 p^{-k-1-n} + \xi_1 p^{-k-2-n} + \cdots + \xi_{n-1} p^{-k-2n} + \cdots =$$

$$\frac{1}{p^k}(\chi_0 p^{k-1} + \chi_1 p^{k-2} + \cdots + \chi_{k-1}) + \frac{1}{p^k} \cdot \frac{\xi_0 p^{n-1} + \xi_1 p^{n-2} + \cdots + \xi_{n-1}}{p^n - 1}, \quad (2.5)$$

where $\chi_i, \xi_j \in \{0, 1, \dots, p-1\}$. Note that in the base- p expansions of rational integers from $[0, 1]$ we use *right*-infinite words rather than left-infinite ones that correspond to canonical expansions of p -adic integers.

Proposition 2.5. *Given $z \in \mathbb{Z}_p \cap \mathbb{Q}$, represent z in the form (2.2); then*

$$z \bmod 1 = 0.(\hat{\beta}_{t-1-\bar{r}} \hat{\beta}_{t-2-\bar{r}} \dots \hat{\beta}_0 \hat{\beta}_{t-1} \hat{\beta}_{t-2} \dots \hat{\beta}_{t-\bar{r}})^\infty \bmod 1,$$

where $\hat{\beta} = p-1-\beta$ for $\beta \in \{0, 1, \dots, p-1\}$ and \bar{r} is the least non-negative residue of r modulo t if $t > 1$ or $\bar{r} = 0$ if otherwise.

Proof. Indeed, by Note 2.3, $\sum_{j=0}^{\infty} p^{r+tj} = -p^r(p^t - 1)^{-1}$ in \mathbb{Z}_p ; so $z = u - vp^r(p^t - 1)^{-1}$ where $u = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1} p^{r-1}$ and $v = \beta_0 + \beta_1 p + \cdots + \beta_{t-1} p^{t-1}$. Therefore

$$z \bmod 1 = \left(-\frac{vp^r}{p^t - 1} \right) \bmod 1.$$

But $(p^t - 1)^{-1} = p^{-t} + p^{-2t} + p^{-3t} + \cdots$ in \mathbb{R} ; so

$$(p^t - 1)^{-1} = 0.\underbrace{(00 \dots 0)}_{t-1} 1)^\infty$$

and thus $-v \cdot (p^t - 1)^{-1} = -0.(\beta_{t-1} \beta_{t-2} \dots \beta_0)^\infty$.

Now just note that

$$(p-1-\gamma_0) + (p-1-\gamma_1)p + \cdots + (p-1-\gamma_{s-1})p^{s-1} = p^s - 1 - (\gamma_0 + \gamma_1 p + \cdots + \gamma_{s-1} p^{s-1})$$

for $\gamma_0, \gamma_1, \dots \in \{0, 1, \dots, p-1\}$, $s \in \mathbb{N}$; so

$$\frac{(p-1-\gamma_0) + (p-1-\gamma_1)p + \dots + (p-1-\gamma_{s-1})p^{s-1}}{p^s - 1} = 1 - \frac{\gamma_0 + \gamma_1 p + \dots + \gamma_{s-1} p^{s-1}}{p^s - 1}$$

and therefore

$$(-0.(\gamma_{s-1}\gamma_{s-2}\dots\gamma_0)^\infty) \bmod 1 = (0.(\hat{\gamma}_{s-1}\hat{\gamma}_{s-2}\dots\hat{\gamma}_0)^\infty) \bmod 1 \quad (2.6)$$

where $\hat{\gamma} = p-1-\gamma$ for $\gamma \in \{0, 1, \dots, p-1\}$. \square

Combining (2.5) with Proposition 2.2 we see that all real numbers whose base- p expansions are purely periodic must lie in $\mathbb{Z}_p \cap \mathbb{Q}$; therefore the following criterion is true:

Corollary 2.6. *A real number x is in $\mathbb{Z}_p \cap \mathbb{Q}$ if and only if base- p expansion of $x \bmod 1$ is purely periodic: $x \bmod 1 = 0.(\chi_0 \dots \chi_{n-1})^\infty$ for suitable $\chi_0, \dots, \chi_{n-1} \in \mathbb{F}_p$.*

The following corollary expresses base- p expansion of a p -adic rational integer via its representation in the form given by Proposition 2.2:

Corollary 2.7. *Once a p -adic rational integer $z \in \mathbb{Z}_p \cap \mathbb{Q}$ is represented in the form as of Proposition 2.2 then $z \bmod 1 = 0.(\zeta_{t-1}\zeta_{t-2}\dots\zeta_0)^\infty$ where $d = \zeta_0 + \zeta_1 p + \dots + \zeta_{t-1} p^{t-1}$.*

Proof. Indeed, under notation of Proposition 2.2, $z \bmod 1 = (d \cdot (p^t - 1)^{-1}) \bmod 1$ and the result follows since $(p^t - 1)^{-1} = p^{-t} + p^{-2t} + p^{-3t} + \dots$ in \mathbb{R} . \square

Now we can find a period length of $z \in \mathbb{Z}_p \cap \mathbb{Q}$ provided z is represented as an irreducible fraction $z = a/b$, where $a \in \mathbb{Z}$, $b \in \mathbb{N}$.

Proposition 2.8. *Once a p -adic rational integer $z \neq 0$ is represented as an irreducible fraction $z = a/b$, and if $b > 1$, then the period length t of z is equal to the multiplicative order of p modulo b (i.e., to the smallest $\ell \in \mathbb{N}$ such that $p^\ell \equiv 1 \pmod{b}$).*

Proof. Note that the multiplicative order ℓ of p modulo b is the smallest positive integer such that $p^\ell(a/b) \equiv a/b \pmod{1}$. Indeed, $p^\ell = eb + 1$ for a suitable $e \in \mathbb{Z}$; so $p^\ell(a/b) = ea + (a/b)$. On the other hand, if $p^s(a/b) = m + (a/b)$ for some $m \in \mathbb{Z}$ then $a(p^s - 1) = mb$ and thus $p^s - 1 \equiv 0 \pmod{b}$ since a is co-prime to b (as the fraction a/b is supposed to be irreducible).

Now, from Corollary 2.7 it immediately follows that $(p^t z) \bmod 1 = z \bmod 1$ once t is a period length of z and that t is the smallest positive integer with that property. Finally we conclude that $\ell = t$. \square

Now given $b \in \mathbb{N}$, b co-prime to p , we denote via $\text{mult}_b p$ the multiplicative order of p modulo b if $b > 1$ or put $\text{mult}_b p = 1$ once $b = 1$. Then $\text{mult}_b p$ is the period length of $z \in \mathbb{Z}_p \cap \mathbb{Q}$ once z is represented as an irreducible fraction $z = a/b$ where $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Note that we consider here only infinite words that correspond to p -adic rational integers; thus to, e.g., 0 there corresponds a word $(0)^\infty$ (so a period of 0 is 0 and a pre-period is empty) and the respective base- p expansion of 0 is $0.(0)^\infty$. Also, $1 = 1 + 0 \cdot p + 0 \cdot p^2 + \dots$, the corresponding infinite word is $(0)^\infty 1$; therefore 1 is a pre-period of 1, 0 is a period of 1, and the representation of 1 in the form (2.3) is $1 = 1 + (0/p - 1)$.

Example 2.9. Let $p = 2$; then $1/3 = 1 \cdot 1 + 1 \cdot 2 + 0 \cdot 4 + 1 \cdot 8 + 0 \cdot 16 + \dots = 1 - 2 \cdot 3^{-1}$ is a canonical 2-adic expansion of $1/3$; so the corresponding infinite binary word is $(01)^\infty 1$. Therefore the period length of $1/3$ is 2 (and note that the multiplicative

order of 2 modulo 3 is indeed 2), the period is 01, the pre-period is 1. Also, $c = 0$ and $d = 1$ once $1/3$ is represented in the form of Proposition 2.2; $1/3 = 0.(01)^\infty$ is a base-2 expansion of $1/3$, cf. Proposition 2.5 and Corollary 2.7.

2.3. Automata: Basics. Here we remind some basic facts from automata theory (see e.g. monographs [8, 9, 15]).

By the definition, a (non-initial) automaton is a 5-tuple $\mathfrak{A} = \langle \mathcal{I}, \mathcal{S}, \mathcal{O}, S, O \rangle$ where \mathcal{I} is a finite set, the *input alphabet*; \mathcal{O} is a finite set, the *output alphabet*; \mathcal{S} is a non-empty (possibly, infinite) set of *states*; $S: \mathcal{I} \times \mathcal{S} \rightarrow \mathcal{S}$ is a *state transition function*; $O: \mathcal{I} \times \mathcal{S} \rightarrow \mathcal{O}$ is an *output function*. An automaton where both input alphabet \mathcal{I} and output alphabet \mathcal{O} are non-empty is called a *transducer*, see e.g. [2, 9]. The *initial automaton* $\mathfrak{A}(s_0) = \langle \mathcal{I}, \mathcal{S}, \mathcal{O}, S, O, s_0 \rangle$ is an automaton \mathfrak{A} where one state $s_0 \in \mathcal{S}$ is fixed; it is called the *initial state*. We stress that the definition of an initial automaton $\mathfrak{A}(s_0)$ is nearly the same as the one of *Mealy automaton* (see e.g. [8, 9]) with the only important difference: the set of states \mathcal{S} of $\mathfrak{A}(s_0)$ is *not necessarily finite*. Note also that in literature the automata we consider in the paper are also referred to as (*letter-to-letter*) *transducers*; in the sequel we use terms ‘automaton’ and ‘transducer’ as synonyms.

Given an input word $w = \chi_{n-1} \cdots \chi_1 \chi_0$ over the alphabet \mathcal{I} , an initial transducer $\mathfrak{A}(s_0) = \langle \mathcal{I}, \mathcal{S}, \mathcal{O}, S, O, s_0 \rangle$ transforms w to output word $w' = \xi_{n-1} \cdots \xi_1 \xi_0$ over the output alphabet \mathcal{O} as follows (cf. Figure 5): Initially the transducer $\mathfrak{A}(s_0)$ is at the state s_0 ; accepting the input symbol $\chi_0 \in \mathcal{I}$, the transducer outputs the symbol $\xi_0 = O(\chi_0, s_0) \in \mathcal{O}$ and reaches the state $s_1 = S(\chi_0, s_0) \in \mathcal{S}$; then the transducer accepts the next input symbol $\chi_1 \in \mathcal{I}$, reaches the state $s_2 = S(\chi_1, s_1) \in \mathcal{S}$, outputs $\xi_1 = O(\chi_1, s_1) \in \mathcal{O}$, and the routine repeats. This way the transducer $\mathfrak{A} = \mathfrak{A}(s_0)$ defines a mapping $\mathfrak{a} = \mathfrak{a}_{s_0}$ of the set $\mathcal{W}_n(\mathcal{I})$ of all n -letter words over the input alphabet \mathcal{I} to the set $\mathcal{W}_n(\mathcal{O})$ of all n -letter words over the output alphabet \mathcal{O} ; thus \mathfrak{A} defines a map of the set $\mathcal{W}(\mathcal{I})$ of all non-empty words over the alphabet \mathcal{I} to the set $\mathcal{W}(\mathcal{O})$ of all non-empty words over the alphabet \mathcal{O} . We will denote the latter map by the same symbol \mathfrak{a} (or by \mathfrak{a}_{s_0} if we want to stress what initial state is meant), and when it is clear from the context what alphabet \mathcal{A} is meant we use notation \mathcal{W} rather than $\mathcal{W}(\mathcal{A})$.

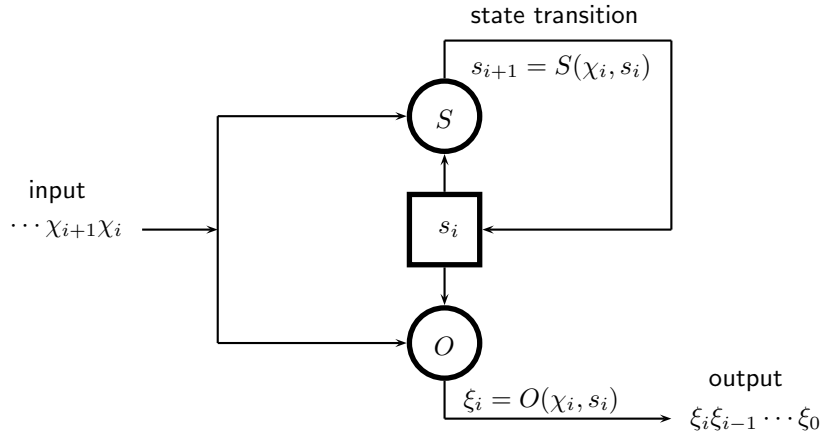


FIGURE 5. Initial transducer, schematically

Throughout the paper, ‘automaton’ mostly stands for ‘initial automaton’; we make corresponding remarks if not. Further in the paper we mostly consider transducers. Furthermore, throughout the paper we consider *reachable transducers* only; that is, we assume that all states of the initial transducer $\mathfrak{A}(s_0)$ are reachable from

the initial state s_0 : Given $s \in \mathcal{S}$, there exists input word w over alphabet \mathcal{I} such that after the word w has been feeded to the automaton $\mathfrak{A}(s_0)$, the automaton reaches the state s . A reachable transducer is called *finite* if its set \mathcal{S} of states is finite, and transducer is called *infinite* if otherwise.

To the initial automaton $\mathfrak{A}(s_0)$ we put into a correspondence a family $\mathcal{F}(\mathfrak{A})$ of all *sub-automata* $\mathfrak{A}(s) = \langle \mathcal{I}, \tilde{\mathcal{S}}, \mathcal{O}, \tilde{S}, \tilde{O}, s \rangle$, $s \in \mathcal{S}$, where $\tilde{\mathcal{S}} = \tilde{\mathcal{S}}(s) \subset \mathcal{S}$ is the set of all states that are reachable from the state s and \tilde{S}, \tilde{O} are respective restrictions of the state transition and output functions S, O on $\mathcal{I} \times \tilde{\mathcal{S}}$. A sub-automaton $\mathfrak{A}(s)$ is called *proper* if the set $\tilde{\mathcal{S}}$ of all its states is a proper subset of \mathcal{S} . A sub-automaton $\mathfrak{A}(s)$ is called *minimal* if it contains no proper sub-automata. It is obvious that a finite sub-automaton is minimal if and only if every its state is reachable from any other its state. The set of all states of a minimal sub-automaton of the automaton \mathfrak{A} is called an *ergodic component* of the (set of all states) of the automaton \mathfrak{A} . It is clear that once the automaton is in a state that belongs to an ergodic component, all its further states will also be in the same ergodic component. Therefore all states of a finite automaton are of two types only: The *transient states* which belong to no ergodic component, and *ergodic states* which belong to ergodic components. It is clear that the set of all ergodic states is a disjoint union of ergodic components. Note that we use the term ‘minimal automaton’ in a different meaning compared to the one used in automata theory, see, e.g., [15]: Our terminology here is from the theory of Markov chains, see, e.g., [21] (since to the graph of state transitions of every automaton there corresponds a Markov chain).

Hereinafter in the paper the word ‘automaton’ stands for a letter-to-letter initial transducer whose input and output alphabet consists of p symbols, and we mostly assume that p is a prime. Thus, for every $n = 1, 2, 3, \dots$ the automaton $\mathfrak{A}(s_0) = \langle \mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0 \rangle$ maps n -letter words over \mathbb{F}_p to n -letter words over \mathbb{F}_p according to the procedure described above, cf. Figure 5. Given two such automata $\mathfrak{A} = \mathfrak{A}(s_0)$ and $\mathfrak{B} = \mathfrak{B}(t_0)$, their *sequential composition* (or briefly, a *composition*) $\mathfrak{C} = \mathfrak{B} \circ \mathfrak{A}$ can be defined in a natural way via sending output of the automaton \mathfrak{A} to input of the automaton \mathfrak{B} so that the mapping $\mathfrak{c}: \mathcal{W} \rightarrow \mathcal{W}$ the automaton \mathfrak{C} performs is just a composite mapping $\mathfrak{b} \circ \mathfrak{a}$ (cf. any of monographs [8, 9, 15] for exact definition and further facts mentioned in the subsection). Note that a composition of finite automata is a finite automaton.

In a similar manner one can consider automata with multiply inputs/outputs; these can be also treated as automata whose input/output alphabets are Cartesian powers of \mathbb{F}_p : For instance, an automaton with m inputs and n outputs over alphabet \mathbb{F}_p can be considered as an automaton with a single input over the alphabet \mathbb{F}_p^m and a single output over the alphabet \mathbb{F}_p^n . Moreover, as the letters of the alphabet \mathbb{F}_p^k are in a one-to-one correspondence with residues modulo p^k ; the automaton with m inputs and n outputs can be considered (if necessary) as an automaton with a single input over the alphabet $\mathbb{Z}/p^m\mathbb{Z}$ and a single output over alphabet $\mathbb{Z}/p^n\mathbb{Z}$. is an automaton with 2 inputs and 1 output which

Compositions of automata with multiple inputs/outputs can also be naturally defined: For instance, given automata $\mathfrak{A}_1, \mathfrak{A}_2$, and \mathfrak{A}_3 with m_1, m_2, m_3 inputs and n_1, n_2, n_3 outputs respectively, in the case when $m_3 = n_1 + n_2$ one can consider a composition of these automata by connecting every output of automata \mathfrak{A}_1 and \mathfrak{A}_2 to some input of the automaton \mathfrak{A}_3 so that every input of the automaton \mathfrak{A}_3 is connected to a unique output which belongs either to \mathfrak{A}_1 or to \mathfrak{A}_2 but not to the both. This way one obtains various compositions of automata \mathfrak{A}_1 and \mathfrak{A}_2 , with the automaton \mathfrak{A}_3 , and either of these compositions is an automaton with $m_1 + m_2$ inputs and n_3 outputs. Moreover, either of the compositions is a finite automaton if all three automata $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3$ are finite.

Automata can be considered as (generally) non-autonomous dynamical systems on different configuration spaces (e.g., \mathcal{W}_n , \mathcal{W} , etc.); the system is autonomous when neither the state transition function \mathcal{S} nor the output function \mathcal{O} depend on input; in this case the automaton is called *autonomous* as well. For purposes of the paper it is convenient to consider automata with input/output alphabets $\mathcal{A} = \mathbb{F}_p$ as dynamical systems on the space \mathbb{Z}_p of p -adic integers, i.e., to relate an automaton \mathfrak{A} to a special map $f_{\mathfrak{A}}: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$. In the next subsection we recall some facts about the map $f_{\mathfrak{A}}$.

2.4. Automata maps: the p -adic view. We identify n -letter words over \mathbb{F}_p with non-negative integers in a natural way: Given an n -letter word $w = \chi_{n-1}\chi_{n-2}\cdots\chi_0$ (i.e., $\chi_i \in \mathbb{F}_p$ for $i = 0, 1, 2, \dots, n-1$), we consider w as a base- p expansion of the number $\text{num}(w) = \chi_0 + \chi_1 \cdot p + \cdots + \chi_{n-1} \cdot p^{n-1} \in \mathbb{N}_0$. In turn, the latter number can be considered as an element of the residue ring $\mathbb{Z}/p^n\mathbb{Z}$ modulo p^n . We denote via wr_n an inverse mapping to num . The mapping wr_n is a bijection of the set $\{0, 1, \dots, p^n - 1\} \subset \mathbb{N}_0$ onto the set \mathcal{W}_n of all n -letter words over \mathbb{F}_p .

As the set $\{0, 1, \dots, p^n - 1\}$ is the set of all non-negative residues modulo p^n , to every automaton $\mathfrak{A} = \mathfrak{A}(s)$ there corresponds a map $f_{n,\mathfrak{A}}$ from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}/p^n\mathbb{Z}$, for every $n = 1, 2, 3, \dots$. Namely, for $r \in \mathbb{Z}/p^n\mathbb{Z}$ put $f_{n,\mathfrak{A}}(r) = \text{num}(\mathfrak{a}(\text{wr}_n(r)))$, where \mathfrak{a} is a word transformation of \mathcal{W}_n performed by the automaton \mathfrak{A} , cf. Subsection 2.3.

Speaking less formally, the mapping $f_{n,\mathfrak{A}}$ can be defined as follows: given $r \in \{0, 1, \dots, p^n - 1\}$, consider a base- p expansion of r , read it as a n -letter word over $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ (put additional zeroes on higher order positions if necessary) and then feed the word to the automaton so that letters that are on lower order positions ('less significant digits') are feeded prior to ones on higher order positions ('more significant digits'). Then read the corresponding output n -letter word as a base- p expansion of a number from \mathbb{N}_0 keeping the same order, i.e. when the earliest outputted letters correspond to lowest order digits in the base- p expansion.

We stress the following determinative property of the mapping $f_{n,\mathfrak{A}}$ which follows directly from the definition: Given $a, b \in \{0, 1, \dots, p^n - 1\}$, whenever $a \equiv b \pmod{p^k}$ for some $k \in \mathbb{N}$ then necessarily $f_{n,\mathfrak{A}}(a) \equiv f_{n,\mathfrak{A}}(b) \pmod{p^k}$. This implication may be re-stated in terms of p -adic metric as follows:

$$|f_{n,\mathfrak{A}}(a) - f_{n,\mathfrak{A}}(b)|_p \leq |a - b|_p. \quad (2.7)$$

Furthermore, every automaton $\mathfrak{A} = \mathfrak{A}(s_0)$ defines a mapping $f_{\mathfrak{A}}$ from \mathbb{Z}_p to \mathbb{Z}_p which can be specified in a manner similar to the one of the mapping $f_{n,\mathfrak{A}}$: Given an infinite word $w = \dots\chi_{n-1}\chi_{n-2}\cdots\chi_0$ (that is, an infinite sequence) over \mathbb{F}_p we consider a p -adic integer whose p -adic canonical expansion is $z = z(w) = \chi_0 + \chi_1 \cdot p + \cdots + \chi_{n-1} \cdot p^{n-1} + \cdots$; so, by the definition, for every $z \in \mathbb{Z}_p$ we put

$$\delta_i(f_{\mathfrak{A}}(z)) = O(\delta_i(z), s_i) \quad (i = 0, 1, 2, \dots), \quad (2.8)$$

where $s_i = S(\delta_{i-1}(z), s_{i-1})$, $i = 1, 2, \dots$, and $\delta_i(z)$ is the i -th p -adic digit of z ; that is, the i -th term coefficient in the p -adic canonical representation of z : $\delta_i(z) = \chi_i \in \mathbb{F}_p$, $i = 0, 1, 2, \dots$ (see Subsection 2.2). The so defined map $f_{\mathfrak{A}}$ is called the *automaton function* (or, the *automaton map*) of the automaton \mathfrak{A} . Note that from (2.8) it follows that

$$\delta_i(f_{\mathfrak{A}}(z)) = \Phi_i(\delta_0(z), \dots, \delta_i(z)), \quad (2.9)$$

where Φ_i is a map from the $(i+1)$ -th Cartesian power \mathbb{F}_p^{i+1} of \mathbb{F}_p into \mathbb{F}_p .

More formally, given $z \in \mathbb{Z}_p$, define $f_{\mathfrak{A}}(z)$ as follows: Consider a sequence $(z \bmod p^n)_{n=1}^{\infty}$ and a corresponding sequence $(f_{n,\mathfrak{A}}(z \bmod p^n))_{n=1}^{\infty}$; then, as the sequence $(z \bmod p^n)_{n=1}^{\infty}$ converges to z w.r.t. p -adic metric (cf. Subsection 2.2), the sequence $(f_{n,\mathfrak{A}}(z \bmod p^n))_{n=1}^{\infty}$ in view (2.7) also converges w.r.t. the p -adic metric (since the

latter sequence is fundamental and \mathbb{Z}_p is closed in \mathbb{Q}_p which is a complete metric space). Now we just put $f_{\mathfrak{A}}(z)$ to be a limit point of the sequence $(f_{n,\mathfrak{A}}(z \bmod p^n))_{n=1}^{\infty}$. Thus, the mapping $f_{\mathfrak{A}}$ is a well-defined function with domain \mathbb{Z}_p and values in \mathbb{Z}_p ; by (2.7) the function $f_{\mathfrak{A}}$ satisfies Lipschitz condition with a constant 1 w.r.t. p -adic metric.

The point is that *the class of all automata functions that correspond to automata with p -letter input/output alphabets coincides with the class of all maps from \mathbb{Z}_p to \mathbb{Z}_p that satisfy the p -adic Lipschitz condition with a constant 1* (the 1-Lipschitz maps, for brevity), cf., e.g., [5]. We note that the claim can also be derived from a more general result on asynchronous automata [18, Proposition 3.7]; for $p = 2$ the claim was proved in [43].

Further we need more detailed information about *finite automata functions*, that is, about functions $f_{\mathfrak{A}}: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ where $\mathfrak{A} = \mathfrak{A}(s_0)$ is a finite automaton (i.e., with a finite set \mathcal{S} of states). It is well known (cf. previous subsection 2.3) that *the class of finite automata functions is closed w.r.t. composition of functions and a sum of functions*: Once $f, g: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ are finite automata functions, either of mappings $x \mapsto f(g(x))$ and $x \mapsto f(x) + g(x)$ ($x \in \mathbb{Z}_p$) is a finite automaton function. Another important property of finite automata functions is that *any finite automaton function maps $\mathbb{Z}_p \cap \mathbb{Q}$ into itself*. In view of (2.2), the latter property is just a re-statement of a well-known property of finite automata which yields that any finite automaton fed by an eventually periodic sequence outputs an eventually periodic sequence, cf., e.g., [8, Corollary 2.6.9], [15, Chapter XIII, Theorem 2.2.]. Since further we often use that property of finite automata, we state it as a lemma for future references:

Lemma 2.10. *If a finite automaton \mathfrak{A} is being fed by a left-infinite periodic word w^{∞} , where $w \in \mathcal{W}$ is a finite non-empty word, then the corresponding output left-infinite word is eventually periodic; i.e., it is of the form $u^{\infty}v$, where $u \in \mathcal{W}$, $v \in \mathcal{W}_{\phi}$. To put it in other words, if a finite automaton is being fed by an eventually periodic finite word $(w)^kt$, where $w \in \mathcal{W}$, $t \in \mathcal{W}_{\phi}$, and $k \in \mathbb{N}$ is sufficiently large, then the output word is of the form $r(u)^{\ell}v$, where $\ell \in \mathbb{N}$, $u \in \mathcal{W}$, $r, v \in \mathcal{W}_{\phi}$ and r is either empty or a prefix of u : $u = hr$ for a suitable $h \in \mathcal{W}_{\phi}$. Therefore the output word is of the form $(\bar{u})^{\ell}v'$, where \bar{u} is a cyclically shifted word u .*

To study finite automata functions it is convenient sometimes to represent 1-Lipschitz maps from \mathbb{Z}_p to \mathbb{Z}_p as special convergent p -adic series, the *van der Put series*. Details about the latter series may be found in, e.g., [31, 38]; here we only briefly recall some basic facts. Given a continuous function $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, there exists a unique sequence B_0, B_1, B_2, \dots of p -adic integers such that

$$f(z) = \sum_{m=0}^{\infty} B_m \chi(m, z) \quad (2.10)$$

for all $z \in \mathbb{Z}_p$, where

$$\chi(m, z) = \begin{cases} 1, & \text{if } |z - m|_p \leq p^{-n} \\ 0, & \text{otherwise} \end{cases}$$

and $n = 1$ if $m = 0$; n is uniquely defined by the inequality $p^{n-1} \leq m \leq p^n - 1$ otherwise. The right side series in (2.10) is called the *van der Put series* of the function f . Note that the sequence $B_0, B_1, \dots, B_m, \dots$ of *van der Put coefficients* of the function f tends p -adically to 0 as $m \rightarrow \infty$, and the series converges uniformly on \mathbb{Z}_p . Vice versa, if a sequence $B_0, B_1, \dots, B_m, \dots$ of p -adic integers tends p -adically to 0 as $m \rightarrow \infty$, then the series in the right part of (2.10) converges uniformly on \mathbb{Z}_p and thus define a continuous function $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$.

The number n in the definition of $\chi(m, z)$ has a very natural meaning; it is just the number of digits in a base- p expansion of $m \in \mathbb{N}_0$:

$$\lfloor \log_p m \rfloor = (\text{the number of digits in a base-}p \text{ expansion for } m) - 1;$$

therefore $n = \lfloor \log_p m \rfloor + 1$ for all $m \in \mathbb{N}_0$ (that is why we assume $\lfloor \log_p 0 \rfloor = 0$).

Note that coefficients B_m are related to the values of the function f in the following way: Let $m = m_0 + \dots + m_{n-2}p^{n-2} + m_{n-1}p^{n-1}$ be a base- p expansion for m , i.e., $m_j \in \{0, \dots, p-1\}$, $j = 0, 1, \dots, n-1$ and $m_{n-1} \neq 0$, then

$$B_m = \begin{cases} f(m) - f(m - m_{n-1}p^{n-1}), & \text{if } m \geq p; \\ f(m), & \text{if otherwise.} \end{cases} \quad (2.11)$$

It worth noticing also that $\chi(m, z)$ is merely a characteristic function of the ball $\mathbf{B}_{p^{-\lfloor \log_p m \rfloor - 1}}(m) = m + p^{\lfloor \log_p m \rfloor - 1} \mathbb{Z}_p$ of radius $p^{-\lfloor \log_p m \rfloor - 1}$ centered at $m \in \mathbb{N}_0$:

$$\chi(m, z) = \begin{cases} 1, & \text{if } z \equiv m \pmod{p^{\lfloor \log_p m \rfloor + 1}}; \\ 0, & \text{if otherwise} \end{cases} = \begin{cases} 1, & \text{if } x \in \mathbf{B}_{p^{-\lfloor \log_p m \rfloor - 1}}(m); \\ 0, & \text{if otherwise} \end{cases} \quad (2.12)$$

Theorem 2.11 (cf. [4]). *A function $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is 1-Lipschitz (that is, an automaton function) if and only if f can be represented as*

$$f(z) = \sum_{m=0}^{\infty} b_m p^{\lfloor \log_p m \rfloor} \chi(m, z), \quad (2.13)$$

where $b_m \in \mathbb{Z}_p$ for $m = 0, 1, 2, \dots$

By using the van der Put series it is possible to determine whether a mapping $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is an automaton function of a finite automaton. We first remind some notions and facts from the theory of automata sequences following [2].

An infinite sequence $\mathbf{a} = (a_i)_{i=0}^{\infty}$ over a finite alphabet \mathcal{A} , $\#\mathcal{A} = L < \infty$, is called *p-automatic* if there exists a finite transducer $\mathfrak{T} = \langle \mathbb{F}_p, \mathcal{S}, \mathcal{A}, S, O, s_0 \rangle$ such that for all $n = 0, 1, 2, \dots$, if \mathfrak{T} is feeded by the word $\chi_k \chi_{k-1} \dots \chi_0$ which is a base- p expansion of $n = \chi_0 + \chi_1 p + \dots + \chi_k p^k$, $\chi_k \neq 0$ if $n \neq 0$, then the k -th output symbol of \mathfrak{T} is a_n ; or, in other words, such that $\delta_k^{\mathcal{A}}(f_{\mathfrak{T}}(n)) = a_n$ for all $n \in \mathbb{N}_0$, where $k = \lfloor \log_p n \rfloor$ and $\delta_k^{\mathcal{A}}(r)$ stands for the k -th digit in the base- L expansion of $r \in \mathbb{N}_0$.

A *p-kernel* of the sequence \mathbf{a} is a set $\ker_p(\mathbf{a})$ of all subsequences $(a_{jp^m+t})_{j=0}^{\infty}$, $m = 0, 1, 2, \dots$, $0 \leq t < p^m$.

Theorem 2.12 (Automaticity criterion, cf. [2, Theorem 6.6.2]). *A sequence \mathbf{a} is p-automatic if and only if its p-kernel is finite.*

Theorem 2.13 (Finiteness criterion, cf. [5]). *Let a 1-Lipschitz function $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ be represented by van der Put series (2.13). The function f is a finite automaton function if and only if the following conditions hold simultaneously:*

- (i) *all coefficients b_m , $m = 0, 1, 2, \dots$, constitute a finite subset $B_f \subset \mathbb{Q} \cap \mathbb{Z}_p$, and*
- (ii) *the p-kernel of the sequence $(b_m)_{m=0}^{\infty}$ is finite.*

Note 2.14. Condition (ii) of the theorem is equivalent to the condition that the sequence $(b_m)_{m=0}^{\infty}$ is *p-automatic*, cf. Theorem 2.12.

Criteria to determine if an automaton function is finite which are based on expansions other than van der Put are also known, cf. [41, 44].

In literature, automata with multiple inputs and outputs over the same alphabet are also studied. We remark that in the case when the alphabet is \mathbb{F}_p , the automata can be considered as automata whose input/output alphabets are Cartesian powers

\mathbb{F}_p^n and \mathbb{F}_p^m , for suitable $m, n \in \mathbb{N}$. For these automata a theory similar to that of automata with a single input/output can be developed: Corresponding automata function are then 1-Lipshitz mappings from \mathbb{Z}_p^n to \mathbb{Z}_p^m w.r.t. p -adic metrics. Recall that p -adic absolute value on \mathbb{Z}_p^k is defined as follows: Given $(z_1, \dots, z_k) \in \mathbb{Z}_p^k$, put $|(z_1, \dots, z_k)|_p = \max\{|z_i|_p : i = 1, 2, \dots, k\}$. The so defined absolute value (and the corresponding metric) are non-Archimedean as well. The main theorem of the paper holds (after a proper re-statement) for these automata as well, see Theorem 5.5.

It is worth recalling here a well-known fact (which also can be proved by using Theorem 2.13) that *addition of two p -adic integers can be performed by a finite automaton with two inputs and one output*: Actually the automaton just finds successively (digit after digit) the sum by a standard addition-with-carry algorithm which is used to find a sum of two non-negative integers represented by base- p expansions thus calculating the sum with arbitrarily high accuracy w.r.t. the p -adic metric. On the contrary, *no finite automaton can perform multiplication of two arbitrary p -adic integers* since it is well known that no finite automaton can calculate a base- p expansion of a square of an arbitrary non-negative integer given a base- p expansion of the latter, cf., e.g., [8, Theorem 2.2.3].

From these remarks combined with Theorem 2.13 the following properties of finite automata functions can be deduced:

Proposition 2.15. *Let $\mathfrak{A}, \mathfrak{B}$ be finite automata, let $a, b \in \mathbb{Z}_p \cap \mathbb{Q}$ be p -adic rational integers. Then the following is true:*

- (i) *the mapping $z \mapsto f_{\mathfrak{A}}(z) + f_{\mathfrak{B}}(z)$ of \mathbb{Z}_p into \mathbb{Z}_p is a finite automaton function;*
- (ii) *a composite function $f(z) = a \cdot f_{\mathfrak{A}}(z) + b$, ($z \in \mathbb{Z}_p$), is a finite automaton function;*
- (iii) *a constant function $f(z) = c$ is a finite automaton function if and only if $c \in \mathbb{Z}_p \cap \mathbb{Q}$;*
- (iv) *an affine mapping $f(z) = c \cdot z + d$ is a finite automaton function if and only if $c, d \in \mathbb{Z}_p \cap \mathbb{Q}$.*

Proof. Note that the van der Put expansion of the constant function $z \mapsto c$ is

$$c = c\chi(0, z) + c\chi(1, z) + \dots + c\chi(p-1, z) + 0\chi(p, z) + 0\chi(p+1, z) + \dots, \quad (2.14)$$

while the van der Put expansion for the identity function $z \mapsto z$ is

$$z = \sum_{i=0}^{\infty} \delta_{[\log_p i]}(i) p^{[\log_p i]} \chi(i, z), \quad (2.15)$$

where $\delta_j(i)$ stands for the j -th digit in the base- p expansion of i . Now all statements of the proposition follow immediately from Theorem 2.13 and the above mentioned facts from finite automata theory. \square

Note that the statement of Proposition 2.15 is known: For instance, it can be deduced from the old work [30] of A. G. Lunts. To our best knowledge, Lunts was the first who revealed connections between automata theory and p -adic analysis. It is worth noticing that Lunts defines automata functions in a slightly different way than we do: In his work, an automaton function is a 1-Lipschitz function $F: \mathbb{Q}_p \rightarrow \mathbb{Q}_p$ such that $F(pz) = pF(z)$ for all $z \in \mathbb{Q}_p$. Also, Lunts' methods of proofs are completely different from the ones of Proposition 2.15. Unfortunately, most automata theorists seem to be unaware of the paper [30] since it was never translated into English and even was never reviewed by Mathematical Reviews.

Concluding the subsection, we remark that in literature (finite) automata functions are also known under names of *(bounded) determinate functions*, or *(bounded) deterministic functions*, cf., e.g., [47, 10, 11, 41].

2.5. Real plots of automata functions vs Monna graphs. Further in the paper we consider special representation of automata functions by point sets of real and complex spaces. As we have already mentioned in previous section, several representations of this sort were considered: Via the so-called limit sets (see e.g. [7]), via the Monna graphs (see e.g. [10, 11, 27, 28, 39]) and via real plots which were originally introduced in [3, Chapter 11]. In the paper we focus on real plots; however we will start this subsection with saying few words about Monna graphs since in some meaning they are counterpart of real plots; and we will not touch limit sets at all since they are standing somewhat apart.

The Monna graphs are based on the Monna's representation of p -adic integers via real numbers of the unit closed segment $[0, 1]$ originally suggested by Monna in [34]: Given a canonical expansion $z = \sum_{i=0}^{\infty} \alpha_i p^i$ of p -adic integer $z \in \mathbb{Z}_p$ (cf. Subsection 2.2), consider a real number $\text{mon}(z) = \sum_{i=0}^{\infty} \alpha_i p^{-i-1} \in [0, 1] \subset \mathbb{R}$. It is clear that mon maps \mathbb{Z}_p onto $[0, 1]$, however, mon is not bijective: The only points from the open interval $(0, 1)$ that have more than one (actually, exactly two) pre-image w.r.t. mon are rational numbers of the form $\sum_{i=0}^{\infty} \alpha_i p^{-i-1}$ where $\alpha_i = p - 1$ for some $i \geq i_0$ since

$$\sum_{i=0}^{\infty} \alpha_i p^{-i-1} = \sum_{i=0}^{\infty} \beta_i p^{-i-1}, \text{ where} \quad (2.16)$$

$$\beta_j = \begin{cases} \alpha_j, & \text{if } j \leq i_0 - 2; \\ (\alpha_{i_0-1} + 1) \bmod p, & \text{if } j = i_0; \\ 0, & \text{if } j \geq i_0 + 1 \end{cases}$$

where $\alpha_j = \beta_j$ for all $j \leq i_0 - 2$, $\beta_j = 0$ for all $j \geq i_0$ and $\beta_{i_0-1} = (\alpha_{i_0-1} + 1) \bmod p$. We can naturally associate the segment $[0, 1]$ (or a half-open interval $[0, 1)$) to the real circle \mathbb{S} by *reducing* $[0, 1]$ *modulo 1*; that is, by taking fractional parts of reals from $[0, 1]$: $\mathbb{S} = [0, 1] \bmod 1$. Then in a similar manner we may consider a mapping of \mathbb{Z}_p onto \mathbb{S} ; we will denote the mapping also via mon since there is no risk of misunderstanding. Note that w.r.t. the latter mapping the point $0 = 1 \in \mathbb{S}$ has exactly two pre-images since $\sum_{i=0}^{\infty} 0 \cdot p^{-i-1} = 0 = 1 = \sum_{i=0}^{\infty} (p-1) \cdot p^{-i-1}$ in \mathbb{S} .

Now, given an automaton $\mathfrak{A} = \mathfrak{A}(s_0)$, we define the *Monna graph* of \mathfrak{A} as follows: Let $f = f_{\mathfrak{A}}$ be a corresponding automaton function, cf. Subsection 2.4 (that is, $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is a 1-Lipschitz function w.r.t. p -adic metric). Then the Monna graph $\mathbf{M}(\mathfrak{A}) = \mathbf{M}(f)$ (or, which is the same, of the automaton function f) is the point set $\mathbf{M}(\mathfrak{A}) = \mathbf{M}(f) = \{(\text{mon}(z), \text{mon}(f(z))) : z \in \mathbb{Z}_p\}$. Note that we can consider the Monna graph when convenient either as a subset of the unit real square \mathbb{I}^2 , a Cartesian square of a unit segment, $\mathbb{I}^2 = [0, 1] \times [0, 1]$, or as a subset of a 2-dimensional real torus $\mathbb{T}^2 = \mathbb{S} \times \mathbb{S}$, a Cartesian square of a real unit circle \mathbb{S} . A Monna graph can be considered as a graph of a real function $f^{\mathfrak{A}}$ defined on $[0, 1]$ and valued in $[0, 1]$. Indeed, given a point $x \in [0, 1]$, which is not of the form (2.16), there is a unique $z \in \mathbb{Z}_p$ such that $\text{mon}(z) = x$. Therefore, $f^{\mathfrak{A}}$ is well defined at x since there exists a unique $y \in [0, 1]$ such that $y = \text{mon}(f_{\mathfrak{A}}(z))$; so we just put $f^{\mathfrak{A}}(x) = y$. Once x is of the form (2.16), then there exist exactly two $z_1, z_2 \in \mathbb{Z}_p$, $z_1 \neq z_2$ such that $\text{mon}(z_1) = \text{mon}(z_2) = x$. As $f_{\mathfrak{A}}(z_1)$ is not necessarily equal to $f_{\mathfrak{A}}(z_2)$, then $f^{\mathfrak{A}}$ may be not well defined at x : One have to assign to $f^{\mathfrak{A}}(x)$ both $\text{mon}(f_{\mathfrak{A}}(z_1))$ and $\text{mon}(f_{\mathfrak{A}}(z_2))$ which may happen to be non-equal. To make $f^{\mathfrak{A}}$ well defined on $[0, 1]$ a usual way is to admit only representations of one (of two) types for x of the form (2.16); say, only those with finitely many non-zero terms,

cf., e.g., [10, 11]. In this case the function $f^{\mathfrak{A}}$ becomes well-defined everywhere on $[0, 1]$ and having points of discontinuity at maybe the points of type (2.16) only. A typical Monna graph of the function $f^{\mathfrak{A}}$ looks like the one represented by Figure 4.

Now we are going to introduce a notion of the *real plot* of an automaton function; the latter notion is somehow ‘dual’ to the notion of Monna graph. Given an automaton $\mathfrak{A} = \mathfrak{A}(s_0)$, we associate to an m -letter non-empty word $v = \gamma_{m-1}\gamma_{m-2}\dots\gamma_0$ over the alphabet \mathbb{F}_p a rational number $0.v$ whose base- p expansion is

$$0.v = 0.\gamma_{m-1}\gamma_{m-2}\dots\gamma_0 = \sum_{i=0}^{m-1} \gamma_{m-i-1}p^{-i-1};$$

then to every m -letter input word $w = \alpha_{m-1}\alpha_{m-2}\dots\alpha_0$ of the automaton \mathfrak{A} and to the respective m -letter output word $\mathfrak{a}(w) = \beta_{m-1}\beta_{m-2}\dots\beta_0$ (rightmost letters are feeded to/outputted from the automaton prior to leftmost ones) there corresponds a point $(0.w; 0.\mathfrak{a}(w))$ of the real unit square \mathbb{I}^2 ; then we define $\mathbf{P}(\mathfrak{A})$ as a closure in \mathbb{R}^2 of the point set $(0.w; 0.\mathfrak{a}(w))$ where w ranges over the set \mathcal{W} of all finite non-empty words over the alphabet \mathbb{F}_p .

Given an automaton function $f = f_{\mathfrak{A}}: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ define a set $\mathbf{P}(f_{\mathfrak{A}})$ of points of the real plane \mathbb{R}^2 as follows: For $k = 1, 2, \dots$ denote

$$E_k(f) = \left\{ \left(\frac{z \bmod p^k}{p^k}; \frac{f(z) \bmod p^k}{p^k} \right) \in \mathbb{I}^2 : z \in \mathbb{Z}_p \right\} \quad (2.17)$$

a point set in a unit real square $\mathbb{I}^2 = [0, 1] \times [0, 1]$ and take a union $E(f) = \bigcup_{k=1}^{\infty} E_k(f)$; then $\mathbf{P}(f)$ is a closure (in topology of \mathbb{R}^2) of the set $E(f)$. Note that if $z = \sum_{i=0}^{\infty} \gamma_i p^i$ is a p -adic canonical expansion of $z \in \mathbb{Z}_p$ then $p^{-m}(z \bmod p^m) = 0.\gamma_{m-1}\gamma_{m-2}\dots\gamma_0$, c.f. (2.17); so $\mathbf{P}(\mathfrak{A}) \supset \mathbf{P}(f_{\mathfrak{A}})$. Moreover, $\mathbf{P}(\mathfrak{A}) = \mathbf{P}(f_{\mathfrak{A}})$, see further Note 2.18.

Definition 2.16 (Automata plots). Given an automaton \mathfrak{A} , we call a *plot of the automaton* \mathfrak{A} the set $\mathbf{P}(\mathfrak{A})$. We call a *limit plot* of the automaton \mathfrak{A} the point set $\mathbf{LP}(\mathfrak{A})$ which is defined as follows: A point $(x; y) \in \mathbb{R}^2$ lies in $\mathbf{LP}(\mathfrak{A})$ if and only if there exist $z \in \mathbb{Z}_p$ and a strictly increasing infinite sequence $k_1 < k_2 < \dots$ of numbers from \mathbb{N} such that simultaneously

$$\lim_{i \rightarrow \infty} \frac{z \bmod p^{k_i}}{p^{k_i}} = x; \quad \lim_{i \rightarrow \infty} \frac{f_{\mathfrak{A}}(z) \bmod p^{k_i}}{p^{k_i}} = y. \quad (2.18)$$

Note 2.17. Further in the paper we consider $\mathbf{LP}(\mathfrak{A})$ (as well as $\mathbf{P}(\mathfrak{A})$ and $\mathbf{P}(f)$) either as a subset of the unit square $\mathbb{I}^2 \subset \mathbb{R}^2$ or as a subset of the unit torus $\mathbb{T}^2 = \mathbb{R}^2/\mathbb{Z}^2$ when appropriate. Note that when considering the plot on the unit torus we reduce coordinates of the points modulo 1, that is, we just ‘glue together’ 0 and 1 of the unit segment \mathbb{I} thus transforming it into the unit circle \mathbb{S} (whose points we usually identify with the points of the half-open segment $[0, 1)$ via a natural one-to-one correspondence, say, $\omega \leftrightarrow \sin^2(\omega/2)$). Also, sometimes we consider $\mathbf{LP}(\mathfrak{A})$ (as well as $\mathbf{P}(\mathfrak{A})$ and $\mathbf{P}(f)$) as a subset of the cylinder $\mathbb{I} \times \mathbb{S}$ or of the cylinder $\mathbb{S} \times \mathbb{I}$ by reducing modulo 1 either y - or x -coordinate respectively. We denote the corresponding plot via $\mathbf{LP}_{\mathbb{M}}(\mathfrak{A})$ by using the subscript $\mathbb{M} \in \{\mathbb{I}^2, \mathbb{T}^2, \mathbb{I} \times \mathbb{S}, \mathbb{S} \times \mathbb{I}\}$ and we omit the subscript when it is clear (or when it is no difference) on which of the surfaces the plot is considered.

We take a moment to recall some well-known topological notions and to introduce some notation. In the sequel, given a subset S of a topological (in particular, metric) space \mathbb{M} which satisfies the Hausdorff axiom we denote via $\mathbf{AP}_{\mathbb{M}}(S)$ the set of all accumulation points of S . Recall that the point $x \in \mathbb{M}$ is called an *accumulation point* of $S \subset \mathbb{M}$ once every neighborhood of x contains infinitely many points from S ; and a point $y \in \mathbb{M}$ is called *isolated point* of S (or, the point isolated from S ;

or, the point isolated w.r.t. S) once there exists a neighborhood $U \ni y$ such that U contains no points from S other than (maybe) y . We may omit the subscript and use notation $\mathbf{AP}(S)$ when it is clear from the context what metric space is meant.

We also write $\mathbf{AP}((a_i)_{i=0}^\infty)$ (or briefly $\mathbf{AP}(a_i)$, or $\mathbf{AP}(\mathcal{C})$) for the set of all limit points of the sequence $\mathcal{C} = (a_i)_{i=0}^\infty$ over \mathbb{M} . Recall that a point $x \in \mathbb{M}$ is called a limit (or, cluster) point of the sequence $(a_i)_{i=0}^\infty$ if every neighbourhood of x contains infinitely many members of the sequence $(a_i)_{i=0}^\infty$; that is, given any neighborhood U of x , the number of i such that $a_i \in U$ is infinite (note that the very $a_i \in U$ are not assumed to be pairwise distinct points of \mathbb{M} ; some, or even all of them may be identical). Note that in topology the terms ‘accumulation point of a set’ and ‘limit point of a set’ are used as synonyms; however to avoid possible misunderstanding we reserve the term ‘limit point’ only for sequences while for sets we use the term ‘accumulation point’.

Note 2.18. The definition of $\mathbf{P}(\mathfrak{A})$ immediately implies that $(x; y) \in \mathbf{P}(\mathfrak{A})$ if and only if there exists a sequence $(w_i)_{i=0}^\infty$ of finite non-empty words $w_i \in \mathcal{W}$ such that $\Lambda(w_i) = k_i$ for all $i = 0, 1, 2, \dots$ and $\lim_{i \rightarrow \infty} \rho(w_i) = x$, $\lim_{i \rightarrow \infty} \rho(\mathfrak{a}(w_i)) = y$. Note that once $(x; y) \in \mathbf{LP}(\mathfrak{A})$ then there exists a sequence $(w_i)_{i=0}^\infty$ of words such that the sequence $(\Lambda(w_i) = k_i)_{i=0}^\infty$ of their lengths is strictly increasing: One just may take $w_i = \text{wr}_{k_i}(z \bmod p^{k_i})$, cf. (2.1) and Subsection 2.4. Therefore $\mathbf{LP}(\mathfrak{A}) \subset \mathbf{AP}(\mathbf{P}(f_{\mathfrak{A}}))$. Moreover, from Definition 2.16 it readily follows that $\mathbf{AP}(\mathbf{P}(f_{\mathfrak{A}})) = \mathbf{AP}(E(f_{\mathfrak{A}})) = \mathbf{AP}(\mathbf{P}(\mathfrak{A}))$ since given a finite non-empty word w and taking any $z \in \mathbb{Z}_p$ such that the prefix of the corresponding infinite word is w (i.e., such that $w = \text{wr}_{\Lambda(w)}(z \bmod p^{\Lambda(w)})$) we see that $\rho(\mathfrak{a}(w)) = ((f_{\mathfrak{A}}(z)) \bmod p^{\Lambda(w)})/p^{\Lambda(w)}$. This implies that $\mathbf{P}(\mathfrak{A}) = \mathbf{P}(f_{\mathfrak{A}})$ since $\mathbf{P}(f_{\mathfrak{A}}) = E(f_{\mathfrak{A}}) \cup \mathbf{AP}(E(f_{\mathfrak{A}})) = \mathbf{P}(\mathfrak{A})$; so in the sequel we do not differ automata plots from the plots of automata functions and use both $\mathbf{P}(\mathfrak{A})$ and $\mathbf{P}(f_{\mathfrak{A}})$ as notation for the plot of the automaton \mathfrak{A} . Also we may use notation $\mathbf{LP}(f_{\mathfrak{A}})$ along with $\mathbf{LP}(\mathfrak{A})$ to denote the limit plot of the automaton \mathfrak{A} .

We stress here once again a crucial difference in the construction of plots and of Monna graphs of automata: Given a canonical expansion of p -adic integer $z = \sum_{i=0}^\infty \gamma_i p^i$ we put into a correspondence to z a *single* real number $\text{mon}(z) = \sum_{i=0}^\infty \gamma_i p^{-i-1}$ while constructing Monna graphs; whereas in the construction of plots we put into a correspondence to z a *whole set of all limit points* of the sequence $(p^{-m}(z \bmod p^m))_{m=1}^\infty$, and the latter set may not consist of a single point; moreover, ‘usually’ the set never consists of a single point since with a probability 1 the set is a whole segment $[0, 1]$. Therefore to study structure of plots we need to work with sets of all limit points of (usually non-convergent) sequences rather than with limits of convergent sequences as in the case of Monna maps.

Proposition 2.19. *Let \mathfrak{A} be an arbitrary automaton; then $\mathbf{LP}(\mathfrak{A})$ contains no points isolated w.r.t. $E(f_{\mathfrak{A}})$ (cf. (2.17) and the text thereafter).*

Proof of Proposition 2.19. Let $(x; y) \in \mathbf{LP}(\mathfrak{A})$ be a point isolated w.r.t. $E(f_{\mathfrak{A}})$. As $(x; y) \in \mathbf{LP}(\mathfrak{A})$, let $z = \sum_{j=0}^\infty \zeta_j \cdot p^j$ be a p -adic canonical representation of the p -adic integer $z \in \mathbb{Z}_p$ mentioned in Definition 2.16; and let $f_{\mathfrak{A}}(z) = \sum_{j=0}^\infty \gamma_j \cdot p^j$ be a p -adic canonical expansion of the p -adic integer $f_{\mathfrak{A}}(z)$. Then as the point $(x; y)$ is isolated, there exists $I \in \mathbb{N}$ such that $z \bmod p^{k_i}/p^{k_i} = x$ and $f_{\mathfrak{A}}(z) \bmod p^{k_i}/p^{k_i} = y$ for all $i \geq I$, cf. (2.18) (if otherwise, the point $(x; y)$ is not isolated w.r.t. $E(f_{\mathfrak{A}})$). Put $w_i = \text{wr}_{k_i}(z \bmod p^{k_i}/p^{k_i}) = \zeta_{k_i-1}\zeta_{k_i-2} \dots \zeta_0$, $u_i = \text{wr}_{k_i}(f_{\mathfrak{A}}(z) \bmod p^{k_i}/p^{k_i}) = \gamma_{k_i-1}\gamma_{k_i-2} \dots \gamma_0$; then

$$0.\zeta_{k_i-1} \dots \zeta_0 = x; \quad (2.19)$$

$$0.\gamma_{k_i-1} \dots \gamma_0 = y, \quad (2.20)$$

for all $i \geq I$. We claim that then necessarily both $z = 0$ and $f_{\mathfrak{A}}(z) = 0$ (whence both $x = 0$ and $y = 0$).

Indeed, as the sequence $\mathcal{K} = (k_i)_{i=0}^{\infty}$ is infinite and strictly increasing, then taking $i = I$ in (2.19) we conclude that necessarily $\zeta_0 = \zeta_1 = \dots = \zeta_{k_{I+M}-k_I-1} = 0$ for all $M \in \mathbb{N}$. Therefore, taking M large enough so that $k_{I+M} - k_I \geq k_I$ (which is always possible since the sequence \mathcal{K} is strictly increasing) we see that $\zeta_0 = \zeta_1 = \dots = \zeta_{k_I-1} = 0$ and thus $\zeta_i = 0$ for all $i \in \mathbb{N}_0$ since $0.\zeta_{k_i-1} \dots \zeta_0 = 0.\zeta_{k_{i-1}-1} \dots \zeta_0$ for all $i \geq I$ by (2.19). But this implies that $z = 0$ (whence $x = 0$). The same argument combined with (2.20) shows that $f_{\mathfrak{A}}(0) = 0$ and $y = 0$.

Consider now an automaton \mathfrak{B} whose automaton function $f_{\mathfrak{B}}$ is defined as follows: Given a p -adic canonical representation $z = \sum_{j=0}^{\infty} \zeta_j \cdot p^j$, let $\delta_0(f_{\mathfrak{B}}(z)) = 1$ and $\delta_j(f_{\mathfrak{B}}(z)) = \delta_j(f_{\mathfrak{A}}(z))$ for $j > 0$. Such an automaton \mathfrak{B} exists since the so defined function $f_{\mathfrak{B}}$ satisfies (2.9) and thus is 1-Lipschitz, cf. Subsection 2.4. Actually the automaton being fed by the input word $\dots \zeta_2 \zeta_1 \zeta_0$ just put 1 as the first output letter and put γ_j for the j -th output letter for $j > 0$ where $\dots \gamma_2 \gamma_1 \gamma_0$ is the output word of the automaton \mathfrak{A} fed by the input word $\dots \zeta_2 \zeta_1 \zeta_0$; that is, \mathfrak{B} outputs $\dots \gamma_2 \gamma_1 1$ being fed by $\dots \zeta_2 \zeta_1 \zeta_0$.

From 2.17 and Definition 2.16 it immediately follows that $\mathbf{LP}(\mathfrak{A}) = \mathbf{LP}(\mathfrak{B})$ and that a point $(x; y) \in \mathbb{R}^2$ is an isolated point of $E(f_{\mathfrak{B}})$ if and only if it is an isolated point of $E(f_{\mathfrak{A}})$. But by the claim we have proved above, once $(x; y)$ is an isolated point of $E(f_{\mathfrak{B}})$, then necessarily $f_{\mathfrak{B}}(0) = 0$. But the first letter of any output word of automaton \mathfrak{B} is 1 by the construction of $f_{\mathfrak{B}}$; thus $\delta_0(f_{\mathfrak{B}}(0)) = 1$ and so $f_{\mathfrak{B}}(0) \neq 0$. From the claim we have proved at the beginning of the proof it follows now that $\mathbf{LP}(\mathfrak{B})$ cannot contain isolated points of $E(f_{\mathfrak{B}})$; thus $\mathbf{LP}(\mathfrak{A})$ cannot contain isolated points of $E(f_{\mathfrak{A}})$. \square

Remark. Note that Proposition 2.19 only states that $\mathbf{LP}(\mathfrak{A})$ contains no points isolated from $E(f_{\mathfrak{A}})$, but of course $\mathbf{LP}(\mathfrak{A})$ may contain isolated points w.r.t. itself. For instance, let \mathfrak{A} be a p -adic odometer; that is, $f_{\mathfrak{A}}(z) = z + 1$ (the automaton \mathfrak{A} may be taken a finite then). Then the point $(1; 0) \in \mathbb{I}^2$ is an isolated point of $\mathbf{LP}_{\mathbb{I}^2}(\mathfrak{A})$ w.r.t. $\mathbf{LP}_{\mathbb{I}^2}(\mathfrak{A})$; however $\mathbf{LP}_{\mathbb{T}^2}(\mathfrak{A})$ contains no points isolated w.r.t. $\mathbf{LP}_{\mathbb{T}^2}(\mathfrak{A})$.

Theorem 2.20. *If automaton \mathfrak{A} is finite and minimal then $\mathbf{AP}(E(f_{\mathfrak{A}})) = \mathbf{LP}(\mathfrak{A})$.*

Proof of Theorem 2.20. By Proposition 2.19, $\mathbf{AP}(E(f_{\mathfrak{A}})) \supset \mathbf{LP}(\mathfrak{A})$; we need to prove that the inverse inclusion also holds. Let $(x; y) \in \mathbf{AP}(E(f_{\mathfrak{A}}))$; then there exists a sequence $(z_i)_{i=0}^{\infty}$ of p -adic integers and a sequence $(k_i)_{i=0}^{\infty}$ of integers from \mathbb{N} such that all the points

$$\mathbf{p}_i = \left(\frac{z_i \bmod p^{k_i}}{p^{k_i}}; \frac{f_{\mathfrak{A}}(z_i) \bmod p^{k_i}}{p^{k_i}} \right) \in \mathbb{R}^2$$

are pairwise distinct and

$$\begin{aligned} \lim_{i \rightarrow \infty} \frac{z_i \bmod p^{k_i}}{p^{k_i}} &= x; \\ \lim_{i \rightarrow \infty} \frac{f_{\mathfrak{A}}(z_i) \bmod p^{k_i}}{p^{k_i}} &= y. \end{aligned}$$

We may assume that the sequence $(k_i)_{i=0}^{\infty}$ is increasing since otherwise in the point sequence $(\mathbf{p}_i)_{i=0}^{\infty}$ there are only finitely many pairwise distinct points. Moreover, we may assume that the sequence $(k_i)_{i=0}^{\infty}$ is strictly increasing; we consider corresponding infinite point subsequence of $(\mathbf{p}_i)_{i=0}^{\infty}$ if otherwise. So we see that there exists an infinite sequence of words $h_i = \text{wr}_{k_i}(z_i \bmod p^{k_i})$ of strictly increasing

lengths k_i such that

$$\lim_{i \rightarrow \infty} 0.h_i = x; \quad (2.21)$$

$$\lim_{i \rightarrow \infty} 0.\mathbf{a}(h_i) = y. \quad (2.22)$$

That is, there exists a sequence $(h_i)_{i=0}^\infty$ of words $h_i = \alpha_{k_i-1}^{(i)} \dots \alpha_0^{(i)}$ of strictly increasing lengths $1 \leq k_0 < k_1 < k_2 < \dots$ such that $\lim_{i \rightarrow \infty} 0.\alpha_{k_i-1}^{(i)} \dots \alpha_0^{(i)} = x$. From here it follows that once i is sufficiently large (say, once $i \geq M_0 \in \mathbb{N}_0$) then $\alpha_{k_i-1}^{(i)} = \zeta_0$ for a suitable $\zeta_0 \in \mathbb{F}_p$. By the same reason, $\alpha_{k_i-2}^{(i)} = \zeta_1$ for a suitable $\zeta_1 \in \mathbb{F}_p$ once i is large enough (say, once $i \geq M_1 \in \mathbb{N}_0$), etc. Moreover, we may assume that the sequence $(M_\ell)_{\ell=0}^\infty$ is strictly increasing. Therefore, $x = 0.\zeta_0\zeta_1\dots$. Applying a similar argument to the sequence $\beta_{k_i-1}^{(i)}\beta_{k_i-2}^{(i)}\dots\beta_0^{(i)} = \mathbf{a}(\alpha_{k_i-1}^{(i)}\alpha_{k_i-2}^{(i)}\dots\alpha_0^{(i)})$ ($i = 0, 1, 2, \dots$) we conclude that there exists a strictly increasing sequence $(N_\ell)_{\ell=0}^\infty$ such that $\beta_{k_i-\ell-1}^{(i)} = \gamma_\ell \in \mathbb{F}_p$ once $i \geq N_\ell$ and therefore $y = 0.\gamma_0\gamma_1\dots$. Moreover, by the construction of the sequences $(M_\ell)_{\ell=0}^\infty$ and $(N_\ell)_{\ell=0}^\infty$ we may assume that $M_\ell = N_\ell$ for all $\ell \in \mathbb{N}_0$. Thus we have shown that

$$\begin{aligned} \alpha_{k_i-1}^{(i)} \dots \alpha_0^{(i)} &= \zeta_0\zeta_1\dots\zeta_\ell w_\ell^{(i)} \text{ if } i \geq M_\ell \ (\ell = 0, 1, 2, \dots); \\ \beta_{k_i-1}^{(i)} \dots \beta_0^{(i)} &= \gamma_0\gamma_1\dots\gamma_\ell u_\ell^{(i)} \text{ if } i \geq M_\ell \ (\ell = 0, 1, 2, \dots), \end{aligned}$$

where $w_\ell^{(i)}, u_\ell^{(i)} \in \mathcal{W}_\phi$ and $\gamma_0\gamma_1\dots\gamma_\ell u_\ell^{(i)} = \mathbf{a}(\zeta_0\zeta_1\dots\zeta_\ell w_\ell^{(i)})$, ($\ell = 0, 1, 2, \dots$). Let $s_\ell^{(i)}$ be a state the automaton \mathfrak{A} reaches after being fed by the input word $w_\ell^{(i)}$ (note that $s_\ell^{(i)} = s_0$, the initial state, once $w_\ell^{(i)}$ is empty word). As the number of states of \mathfrak{A} is finite, at least one state $s \in \mathcal{S}$ repeats in the sequence $(s_\ell^{(M_\ell)})_{\ell=0}^\infty$ infinitely many times. Therefore

$$\lim_{\ell \rightarrow \infty} 0.\zeta_0\dots\zeta_\ell = x; \text{ whence } x = 0.\zeta_0\zeta_1\zeta_2\dots \quad (2.23)$$

$$\lim_{\ell \rightarrow \infty} 0.\mathbf{a}_s(\zeta_0\dots\zeta_\ell) = y; \text{ whence } y = 0.\gamma_0\gamma_1\gamma_2\dots \quad (2.24)$$

Denote $w_\ell = \zeta_0\dots\zeta_\ell$, $v_\ell = \gamma_0\dots\gamma_\ell$, ($\ell = 0, 1, 2, \dots$). As every state of the automaton \mathfrak{A} is reachable from the initial state s_0 , there exists a word $t_0 \in \mathcal{W}_\phi$ such that if the automaton \mathfrak{A} (which is initially at the state s_0) has been fed by the word t_0 , then \mathfrak{A} outputs the word $\bar{t}_0 = \mathbf{a}(t_0)$ and reaches the state s . Thus $\mathbf{a}(w_0 t_0) = \gamma_0 \bar{t}_0$, and the automaton \mathfrak{A} after being fed by the word $w_0 t_0$ reaches the state $r^{(0)}$. As the automaton \mathfrak{A} is minimal, there exists a word $t_1 \in \mathcal{W}_\phi$ such that once the automaton $\mathfrak{A}_1 = \mathfrak{A}(r^{(0)})$ has been fed by the word t_1 , the automaton reaches the state s . Now being fed by the word w_1 , the automaton $\mathfrak{A}_s = \mathfrak{A}(s)$ outputs the word v_1 and reaches a state $r^{(1)}$. By the minimality of \mathfrak{A} , there exists a word $t_2 \in \mathcal{W}_\phi$ such that after $\mathfrak{A}(r^{(1)})$ has been fed by the word t_2 , the automaton reaches the state s . Now after \mathfrak{A}_s has been fed by the word w_2 , the automaton \mathfrak{A}_s reaches the state $r^{(2)}$, and we can find a word t_3 in a manner similar to that of described. Now being fed by the so constructed left-infinite word $\dots w_2 t_2 w_1 t_1 w_0 t_0$, the automaton \mathfrak{A} outputs the left-infinite word $\dots v_2 \bar{t}_2 v_1 \bar{t}_1 v_0 \bar{t}_0$ where $\bar{t}_j = \mathbf{a}_{r^{(j-1)}}(t_j)$, $j = 1, 2, 3, \dots$. Now consider p -adic integers $z = \sum_{i=0}^\infty \chi_i \cdot p^i$ and $\bar{z} = \sum_{i=0}^\infty \xi_i \cdot p^i$ which correspond to infinite words $\dots w_2 t_2 w_1 t_1 w_0 t_0$ and $\dots v_2 \bar{t}_2 v_1 \bar{t}_1 v_0 \bar{t}_0$ accordingly; that is, $\dots \chi_2 \chi_1 \chi_0 = \dots w_2 t_2 w_1 t_1 w_0 t_0$ and $\dots \xi_2 \xi_1 \xi_0 = \dots v_2 \bar{t}_2 v_1 \bar{t}_1 v_0 \bar{t}_0$. Then, by the

construction we have that $\bar{z} = f_{\mathfrak{A}}(z)$, and from (2.23)–(2.24) it follows that

$$\lim_{j \rightarrow \infty} \frac{z \bmod p^{K_j}}{p^{K_j}} = x; \quad (2.25)$$

$$\lim_{j \rightarrow \infty} \frac{f_{\mathfrak{A}}(z) \bmod p^{K_j}}{p^{K_j}} = y, \quad (2.26)$$

where $K_j = \sum_{i=0}^j \Lambda(w_i) + \sum_{i=0}^j \Lambda(t_i)$. As the sequence $(K_j)_{j=0}^{\infty}$ is strictly increasing, from (2.25)–(2.26) it follows now that $(x; y) \in \mathbf{LP}(\mathfrak{A})$ in view of Definition 2.16. \square

It is well known (see e.g. [1, Ch.2, Exercise 2]) that the set of all accumulation points of a Hausdorff topological space (the *derived set* of the space) is a closed subset of the space. From Theorem 2.20 it follows that once a finite automaton is minimal then its limit plot is a derived set of its plot (whence, closed):

Corollary 2.21. *Let an automaton \mathfrak{A} be finite and minimal; then the set $\mathbf{LP}(\mathfrak{A})$ is a derived set of $\mathbf{P}(\mathfrak{A})$ and therefore is closed in \mathbb{R}^2 . A point $(x; y) \in \mathbb{R}^2$ belongs to $\mathbf{LP}(\mathfrak{A})$ if and only if there exists a sequence $(\alpha_{k_i-1}^{(i)} \dots \alpha_0^{(i)})_{i=0}^{\infty}$ of finite non-empty words of strictly increasing lengths $k_0 < k_1 < k_2 < \dots$ such that the sequence $(0.\alpha_{k_i-1}^{(i)} \alpha_{k_i-2}^{(i)} \dots \alpha_0^{(i)})_{i=0}^{\infty}$ tends to x and the corresponding sequence $(0.\beta_{k_i-1}^{(i)} \beta_{k_i-2}^{(i)} \dots \beta_0^{(i)})_{i=0}^{\infty}$ tends to y as $i \rightarrow \infty$, where $\beta_{k_i-1}^{(i)} \dots \beta_0^{(i)}$ are respective output words of the automaton \mathfrak{A} that correspond to input words $\alpha_{k_i-1}^{(i)} \dots \alpha_0^{(i)}$ (i.e., $\beta_{k_i-1}^{(i)} \beta_{k_i-2}^{(i)} \dots \beta_0^{(i)} = \mathbf{a}(\alpha_{k_i-1}^{(i)} \alpha_{k_i-2}^{(i)} \dots \alpha_0^{(i)})$, $i = 0, 1, 2, \dots$).*

We stress once again that words $\alpha_{k_i-1} \dots \alpha_0$ are feeded to the automaton \mathfrak{A} from right to left; i.e. the letter α_0 is feeded to \mathfrak{A} first, then the letter α_1 is feeded to \mathfrak{A} , etc.

Proof of Corollary 2.21. By the definition, the set $\mathbf{AP}(E(f_{\mathfrak{A}})) = \mathbf{AP}(\mathbf{P}(\mathfrak{A}))$ is a derived set of $\mathbf{P}(\mathfrak{A})$; whence by Theorem 2.20 the set $\mathbf{LP}(\mathfrak{A})$ is a derived (thus, closed) set of $\mathbf{P}(\mathfrak{A})$.

The necessity of conditions of the corollary follows immediately from Definition 2.16 since once $(x; y) \in \mathbf{LP}(\mathfrak{A})$ then there exist a p -adic integer $z = \sum_{i=0}^{\infty} \alpha_i \cdot p^i$ and a strictly increasing sequence $1 \leq k_1 < k_2 < \dots$ over \mathbb{N} such that (2.18) holds; that is, we just put $\alpha_{k_i-1}^{(i)} \dots \alpha_0^{(i)} = \text{wr}_{k_i}(z \bmod p^{k_i})$ and $\beta_{k_i-1}^{(i)} \dots \beta_0^{(i)} = \text{wr}_{k_i}(f(z) \bmod p^{k_i})$, where f is an automaton function of \mathfrak{A} , cf. Note 2.18.

To prove sufficiency of the conditions note that the conditions just yield that there exists an infinite sequence of words $h_i = \alpha_{k_i-1}^{(i)} \dots \alpha_0^{(i)}$ of strictly increasing lengths k_i such that (2.21)–(2.22) hold. The argument that follows (2.21)–(2.22) of the proof of Theorem 2.20 now proves the sufficiency. \square

It is worth noticing here that the limit plot of a finite minimal automaton does not depend on what state of the automaton is taken as initial:

Note 2.22. If s, t are states of a finite minimal automaton \mathfrak{A} , $s \neq t$, then $\mathbf{LP}(\mathfrak{A}(s)) = \mathbf{LP}(\mathfrak{A}(t))$.

Indeed, due to the minimality, every state of \mathfrak{A} is reachable from any other state of \mathfrak{A} . Therefore if $(x; y) \in \mathbf{LP}(\mathfrak{A}(t))$ then by Definition 2.16 there exist $z \in \mathbb{Z}_p$ and a strictly increasing infinite sequence $k_1 < k_2 < \dots$ of numbers from \mathbb{N} such that (2.18) holds. By the minimality of \mathfrak{A} , there exists a finite word w of length $K > 0$ such that after the automaton $\mathfrak{A}(s)$ has been feeded by w , it reaches the state t . Now

by substituting in Definition 2.16 $p^K \cdot z + \text{num}(w)$ for z and $k_1 + K < k_2 + K < \dots$ for $k_1 < k_2 < \dots$ we see that (2.18) holds and therefore $(x; y) \in \mathbf{LP}(\mathfrak{A}(s))$.

Using an idea similar to that of Note 2.22 it can be easily demonstrated that if \mathfrak{B} is a sub-automaton of \mathfrak{A} then $\mathbf{P}(\mathfrak{B}) \subset \mathbf{P}(\mathfrak{A})$ since every state of the automaton \mathfrak{A} is reachable from its initial state:

Note 2.23. Let $\mathfrak{B} = \mathfrak{B}(s)$ be a sub-automaton of the automaton \mathfrak{A} . As the initial state s of the automaton \mathfrak{B} is reachable from the initial state s_0 of the automaton \mathfrak{A} , from the definition of the respective sets it immediately follows that $\mathbf{P}(\mathfrak{B}) \subset \mathbf{P}(\mathfrak{A})$, $\mathbf{LP}(\mathfrak{B}) \subset \mathbf{LP}(\mathfrak{A})$, and $\mathbf{AP}(\mathfrak{B}) \subset \mathbf{AP}(\mathfrak{A})$.

The following useful lemma is a sort of a counter-part of Lemma 2.10 in terms of points from $\mathbf{LP}(\mathfrak{A})$ rather than in terms of words.

Lemma 2.24. *Given a finite automaton \mathfrak{A} and a point $x \in \mathbb{Z}_p \cap \mathbb{Q}$, if $(x; y) \in \mathbf{LP}(\mathfrak{A})$ for some $y \in \mathbb{R}$ then $y \in \mathbb{Z}_p \cap \mathbb{Q}$.*

Proof of Lemma 2.24. As $(x; y) \in \mathbf{LP}(\mathfrak{A})$ then there exist $z \in \mathbb{Z}_p$ and a strictly increasing sequence $k_0 < k_1 < \dots$ over \mathbb{N} such that (2.18) holds. Therefore there exists an infinite sequence of words $h_i = \text{wr}_{k_i}(z \bmod p^{k_i})$ of strictly increasing lengths k_i such that (2.21)–(2.22) hold simultaneously. Now repeating for the case $z_i = z$ the argument that follows (2.21)–(2.22) in the proof of Theorem 2.20 we conclude that (2.23)–(2.24) hold in our case as well (note that nowhere in the mentioned argument from the proof of Theorem 2.20 we used that \mathfrak{A} is minimal). Moreover, in the notation of the argument, there exists a strictly increasing sequence $(M_\ell)_{\ell=0}^\infty$ over \mathbb{N} such that

$$\alpha_{k_i-1}^{(i)} \dots \alpha_0^{(i)} = \zeta_0 \zeta_1 \dots \zeta_\ell w_\ell^{(i)} \text{ if } i \geq M_\ell \ (\ell = 0, 1, 2, \dots); \quad (2.27)$$

$$\beta_{k_i-1}^{(i)} \dots \beta_0^{(i)} = \gamma_0 \gamma_1 \dots \gamma_\ell u_\ell^{(i)} \text{ if } i \geq M_\ell \ (\ell = 0, 1, 2, \dots); \quad (2.28)$$

But $\alpha_j^{(i)}, \beta_j^{(i)}$ do not depend on i since in our case $z_i = z = \sum_{n=0}^\infty \alpha_n p^n$ (where $\alpha_0, \alpha_1, \dots \in \mathbb{F}_p$) for all i ; therefore $\alpha_n^{(i)} = \alpha_n$ for all $n, i \in \mathbb{N}_0$. As $x = 0.\zeta_0 \zeta_1 \dots$ (cf. (2.23)) and $x \in \mathbb{Z}_p \cap \mathbb{Q}$ then the right-infinite word $\zeta_0 \zeta_1 \dots$ must be purely periodic (cf. Corollary 2.6) with a period $\chi_0 \dots \chi_{t-1}$ of length $t > 0$: that is, $\zeta_0 \zeta_1 \dots = (\chi_0 \dots \chi_{t-1})^\infty$. Now in (2.27) put $\ell = mt - 1$; then for every $m \in \mathbb{N}$ we have that $\alpha_{k_i-1} \dots \alpha_{k_i-mt} = (\chi_0 \dots \chi_{t-1})^m$ for all $i \geq M_{mt}$. Now denote via $s_m^{(i)}$ the state the automaton \mathfrak{A} reaches after have been feeded by the word $w_{mt}^{(i)}$. Fix $m \in \mathbb{N}$ and denote s_m a state which occurs in the sequence $(w_{mt}^{(i)})_{i=M_{mt}}^\infty$ infinitely often; due to the finiteness of the automaton \mathfrak{A} such state exists. Denote K_m the smallest $i \geq M_{mt}$ such that $s_m = s_m^{(i)}$ (therefore $K_m \geq M_{mt}$). And again due to the finiteness of the automaton \mathfrak{A} in the sequence $(s_m)_{m=1}^\infty$ some state (say, s) occurs infinitely often. Let $(m_j)_{j=0}^\infty$ be the corresponding infinite (thus, strictly increasing) subsequence, i.e., $s_{m_j} = s$; then as the sequence $(M_\ell)_{\ell=0}^\infty$ is strictly increasing and as $K_m \geq M_{mt}$, in the sequence $(K_{m_j})_{j=0}^\infty$ there exists a strictly increasing subsequence, say $(K_{m_{j_r}})_{r=0}^\infty$ (note that the sequence $(m_{j_r})_{r=0}^\infty$ is also strictly increasing). Now from (2.27)–(2.28) it follows that once being feeded successfully by purely periodic words $w_r = \alpha_{k_i-1} \dots \alpha_{k_i-m_{j_r}t} = (\chi_0 \dots \chi_{t-1})^{m_{j_r}}$ for $i = K_{m_{j_r}}$, $r = 0, 1, 2, \dots$, the automaton $\mathfrak{A}(s)$ outputs the words $v_r = \gamma_0 \gamma_1 \dots \gamma_{t \cdot m_{j_r}-1}$. Now by combining Lemma 2.10 with Corollary 2.6 we conclude that if $z' \in \mathbb{Z}_p$ is such that $\text{wr}_{j_r} z' = (\chi_0 \dots \chi_{t-1})^\infty$ then $\lim_{r \rightarrow \infty} (z' \bmod p^{m_{j_r}}) / p^{m_{j_r}} = x$ and $\lim_{r \rightarrow \infty} ((\alpha_s(z')) \bmod p^{m_{j_r}}) / p^{m_{j_r}} = y \in \mathbb{Z}_p \cap \mathbb{Q}$. \square

Yet one more property of automata plots is their invariance with respect to p -shifts. That is, given a point $(x; y) \in \mathbf{P}(\mathfrak{A})$, take base- p expansions $x = 0.\chi_1 \chi_2 \chi_3 \dots$,

$y = 0.\xi_1\xi_2\xi_3\dots$ of coordinates x, y ; then $(0.\chi_2\chi_3\dots; 0.\xi_2\xi_3\dots) \in \mathbf{P}(\mathfrak{A})$. To put it in other words, the following proposition is true:

Proposition 2.25. *For an arbitrary automaton \mathfrak{A} , if $(x; y) \in \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^2$ (resp., $(x; y) \in \mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$) then $((px) \bmod 1; (py) \bmod 1) \in \mathbf{P}(\mathfrak{A})$ (resp., $((px) \bmod 1; (py) \bmod 1) \in \mathbf{LP}(\mathfrak{A})$).*

Proof of Proposition 2.25. The first statement follows immediately from Note 2.18 since once

$$(0.\alpha_{k_i}\dots\alpha_0; 0.\beta_{k_i}\dots\beta_0) \rightarrow (0.\chi_1\chi_2\dots; 0.\xi_1\xi_2\dots)$$

as $i \rightarrow \infty$ then necessarily

$$(0.\alpha_{k_i-1}\dots\alpha_0; 0.\beta_{k_i-1}\dots\beta_0) \rightarrow (0.\chi_2\chi_3\dots; 0.\xi_2\xi_3\dots)$$

as $i \rightarrow \infty$.

To prove the second statement, let $f = f_{\mathfrak{A}}: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ be an automaton function of the automaton \mathfrak{A} . As $(x; y) \in \mathbf{LP}(\mathfrak{A})$, there exists $z \in \mathbb{Z}_p$ and a strictly increasing sequence $(k_i)_{i=0}^\infty$ over \mathbb{N} such that $x = \lim_{i \rightarrow \infty} (z \bmod p^{k_i})/p^{k_i}$ and $y = \lim_{i \rightarrow \infty} (f(z) \bmod p^{k_i})/p^{k_i}$, cf. Definition 2.16. Therefore $(px) \bmod 1 = (p \lim_{i \rightarrow \infty} (z \bmod p^{k_i})/p^{k_i}) \bmod 1 = \lim_{i \rightarrow \infty} (p(z \bmod p^{k_i})/p^{k_i}) \bmod 1 = \lim_{i \rightarrow \infty} (z \bmod p^{k_i-1})/p^{k_i-1}$ as $(z \bmod p^{k_i})/p^{k_i} = \zeta_{k_i-1}p^{-1} + \zeta_{k_i-2}p^{-2} + \dots + \zeta_0p^{-k_i}$ once $z = \zeta_0 + \zeta_1p + \dots + \zeta_{k_i-1}p^{k_i-1} + \dots$ is a p -adic canonical representation for $z \in \mathbb{Z}_p$. By the same reason, $(py) \bmod 1 = (p \lim_{i \rightarrow \infty} (f(z) \bmod p^{k_i})/p^{k_i}) \bmod 1 = \lim_{i \rightarrow \infty} (p(f(z) \bmod p^{k_i})/p^{k_i}) \bmod 1 = \lim_{i \rightarrow \infty} (f(z) \bmod p^{k_i-1})/p^{k_i-1}$. Therefore $((px) \bmod 1; (py) \bmod 1) \in \mathbf{LP}(\mathfrak{A})$ by Definition 2.16. \square

It is known that the plot $\mathbf{P}(\mathfrak{A}) \subset \mathbb{I}^2$ of the automaton \mathfrak{A} can be of two types only; namely, *given an automaton \mathfrak{A} , the set $\mathbf{P}(\mathfrak{A})$ either coincides with the whole unit square \mathbb{I}^2 or $\mathbf{P}(\mathfrak{A})$ is nowhere dense in \mathbb{I}^2* : Being closed in \mathbb{R}^2 , the set $\mathbf{P}(\mathfrak{A})$ is measurable w.r.t. Lebesgue measure on \mathbb{R}^2 , and the measure of $\mathbf{P}(\mathfrak{A})$ is 1 if and only if $\mathbf{P}(\mathfrak{A}) = \mathbb{I}^2$ and is 0 if otherwise: The later assertion is a statement of automata 0-1 law, cf. [3, Proposition 11.15] and [6]. Moreover, *once an automaton \mathfrak{A} is finite, the measure of $\mathbf{P}(\mathfrak{A})$ is 0 and $\mathbf{P}(\mathfrak{A})$ is nowhere dense in \mathbb{I}^2 (cf. op. cit.)*. Therefore, *plots of finite automata are Lebesgue measure 0 nowhere dense closed subsets of the unit square \mathbb{I}^2* ; thus they can not contain sets of positive measure, but they may contain lines. The goal of the paper is to prove that if \mathfrak{A} is a finite automaton then smooth curves which lies completely in $\mathbf{P}(\mathfrak{A})$ (thus in $\mathbf{LP}(\mathfrak{A})$, cf. further Theorem 5.1) can only be straight lines. Moreover, we will prove that *if finite automata plots are considered as subsets of the unit torus \mathbb{T}^2 in \mathbb{R}^3 then smooth curves lying in the plots can only be torus windings*. For this purpose we will need some extra information (which follows) about torus knots.

2.6. Torus knots, torus links and linear flows on torus. Further in the paper we will need only few concepts concerning torus knots theory; details may be found in numerous books on knot theory, see e.g. [12, 32]. For our purposes it is enough to recall only two notions, the knot and the link. Recall that a knot is a smooth embedding of a circle \mathbb{S} into \mathbb{R}^3 and a link is a smooth embedding of several disjoint circles in \mathbb{R}^3 , cf. [32]. We will consider only special types of knots and links, namely, torus knots and torus links. Informally, a torus knot is a smooth closed curve without intersections which lies completely in the surface of a torus $\mathbb{T}^2 \subset \mathbb{R}^3$, and a link (of torus knots) is a collection of (possibly knotted) torus knots, see e.g. [14, Section 26] for formal definitions.

We also need a notion of a cable of torus. Formally, a cable of torus is any geodesic on torus. Recall that geodesics on torus \mathbb{T}^2 are images of straight lines in \mathbb{R}^2 under the mapping $(x; y) \mapsto (x \bmod 1; y \bmod 1)$ of \mathbb{R}^2 onto $\mathbb{T}^2 = \mathbb{R}^2/\mathbb{Z} \times \mathbb{Z}$, cf., e.g., [33, Section 5.4].

Definition 2.26 (Cable of the torus). A *cable of the torus* is an image of a straight line in \mathbb{R}^2 under the map $\text{mod}1: (x; y) \mapsto (x \bmod 1; y \bmod 1)$ of the Euclidean plane \mathbb{R}^2 onto the 2-dimensional real torus $\mathbb{T}^2 = \mathbb{R}^2/\mathbb{Z} \times \mathbb{Z} = \mathbb{S} \times \mathbb{S} \subset \mathbb{R}^3$. If the line is defined by the equation $y = ax + b$ we say that a is a *slope* of the cable $\mathbf{C}(a, b)$. We denote via $\mathbf{C}(\infty, b)$ a cable which corresponds to the line $x = b$, the *meridian*, and say that the slope is ∞ in this case. Cables $\mathbf{C}(0, b)$ of slope 0 (i.e., the ones that correspond to straight lines $y = b$) are called *parallels*.

In dynamics, cables of torus \mathbb{T}^2 are viewed as orbits of *linear flows on torus*; that is, of dynamical systems on \mathbb{T}^2 defined by a pair of differential equations of the form $\frac{dx}{dt} = \beta; \frac{dy}{dt} = \alpha$ on \mathbb{T}^2 , whence, by a pair of parametric equations $x = (\beta t + \tau) \bmod 1; y = (\alpha t + \sigma) \bmod 1$ in Cartesian coordinates, cf. e.g. [19, Subsection 4.2.3].

Note 2.27. It is well known that a cable defined by the straight line $y = ax + b$ is dense in \mathbb{T}^2 if and only if $-\infty < a < +\infty$ and the slope $a = \frac{\alpha}{\beta}$ is irrational, see e.g. [19, Proposition 4.2.8] or [33, Section 5.4].

Given a Cartesian coordinate system XYZ of \mathbb{R}^3 , a torus can be obtained by rotation around Z -axis of a circle which lies in the plane XZ . If a radius of the circle is r and the circle is centered at a point lying in X -axis at a distance R from the origin, then in cylindrical coordinates (r_0, θ, z) of \mathbb{R}^3 (where r_0 is a radius-vector in Cartesian coordinate system XY , θ is an angle of the radius-vector in coordinates XY , z is a Z -coordinate in Cartesian coordinate system XYZ) the torus is defined by the equation $(r_0 - R)^2 + z^2 = r^2$ and a cable (with a rational slope $\frac{\alpha}{\beta}$ where $\alpha \in \mathbb{Z}$ and $\beta \in \mathbb{N}$) of the torus is defined by the system of parametric equations (with parameter $t \in \mathbb{R}$) of the form

$$\begin{bmatrix} r_0 \\ \theta \\ z \end{bmatrix} = \begin{bmatrix} R + r \cos\left(\frac{\alpha}{\beta}t + \omega\right) \\ t \\ r \sin\left(\frac{\alpha}{\beta}t + \omega\right) \end{bmatrix}, \quad t \in \mathbb{R}. \quad (2.29)$$

The cable defined by the above equations winds β times around Z -axis and $|\alpha|$ times around a circle in the interior of the torus (the sign of α determines whether the rotation is clockwise or counter-clockwise), see for an example of the corresponding torus knot Figures 6 and 7 where $\alpha = 5$ and $\beta = 3$. Letting ω in the above equations take a finite number of values we get an example of torus link, see e.g. Figures 10 and 11 which illustrate a link consisting of a pair of torus knots whose slopes are $\frac{3}{5}$. Note that Figures 12 and 13 illustrate a union of two distinct torus links (of two and of three knots respectively) rather than a single torus link of 5 knots. Finally, due to the above representation of a torus link in the form of equations in cylindrical coordinates, we naturally associate the torus link consisting of N cables with slopes $\frac{\alpha}{\beta}$ to a family of complex-valued functions $\psi_k: \mathbb{R} \rightarrow \mathbb{C}$ of real variable $t \in \mathbb{R}$

$$\left\{ \psi_j(t) = e^{i(\frac{\alpha}{\beta}t + \omega_j)} : j = 0, 1, 2, \dots, N-1 \right\},$$

where i stands for imaginary unit $i \in \mathbb{C}: i^2 = -1$.

3. PLOTS OF FINITE AUTOMATON FUNCTIONS: CONSTANT AND AFFINE CASES

In this section we completely describe limit plots of finite automata maps of the forms $z \mapsto c$ (constant maps), $z \mapsto az$ (linear maps) and $z \mapsto az + b$ (affine maps), where a, b, c are some (suitable) p -adic integers and the variable z takes values in \mathbb{Z}_p .

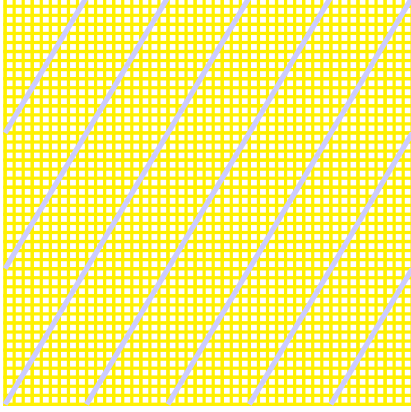


FIGURE 6. A limit plot of the function $f(z) = \frac{5}{3}z$, $z \in \mathbb{Z}_2$, in \mathbb{R}^2

FIGURE 7. A limit plot of the same function on the torus \mathbb{T}^2

3.1. Limit plots of constants. Recall that an automaton $\mathfrak{A}(s_0) = \langle \mathcal{J}, \mathcal{S}, \mathcal{O}, S, O, s_0 \rangle$ is called *autonomous* once neither its state update function S nor its output function O depend on input; i.e., when $s_{i+1} = S(s_i)$, $\xi_i = O(\chi_i, s_i) = O(s_i)$ ($i = 0, 1, 2, \dots$), cf. Fig. 5.

It is clear that an autonomous automaton function is a constant; however a limit plot of this function is not necessarily a straight line. For instance, the limit plot of a constant $c \in \mathbb{Z}_p$ is the whole unit square \mathbb{I}^2 once $c = \sum_{i=0}^{\infty} \alpha_i p^i$ where the infinite word $u = \dots \alpha_2 \alpha_1 \alpha_0$ over \mathbb{F}_p is such that every non-empty finite word $w = \gamma_{k-1} \gamma_{k-2} \dots \gamma_0$ over \mathbb{F}_p occurs as a subword in u ; that is, if there exist a finite word v and an infinite word s over \mathbb{F}_p such that u is a concatenation of v , w and s : $u = svw$, cf. [6].

On the other hand, once an autonomous automaton \mathfrak{A} is finite, the corresponding infinite output word must necessarily be eventually periodic. That is, $c = \alpha_0 + \alpha_1 p + \dots + \alpha_{r-1} p^{r-1} + (\beta_0 + \beta_1 p + \dots + \beta_{t-1} p^{t-1}) \cdot \sum_{j=0}^{\infty} p^{r+tj}$ for suitable $\alpha_i, \beta_j \in \mathbb{F}_p$; therefore a finite autonomous automaton function is a rational constant, i.e., $c \in \mathbb{Z}_p \cap \mathbb{Q}$, cf. Propositions 2.1 and 2.15.

Furthermore, the numbers that correspond to (sufficiently long) finite output words are then all the form

$$0.\beta_k \beta_{k-1} \dots \beta_0 \beta_{t-1} \beta_{t-2} \dots \beta_0 \beta_{t-1} \beta_{t-2} \dots \beta_0 \dots \beta_{t-1} \beta_{t-2} \dots \beta_0 \alpha_{r-1} \alpha_{r-2} \dots \alpha_0$$

for $k = 0, 1, \dots, t-1$. Consequently, the limit plot of the automaton (in \mathbb{R}^2) consists of t pairwise parallel straight lines which correspond to the numbers

$$0.\beta_k \beta_{k-1} \dots \beta_0 \beta_{t-1} \beta_{t-2} \dots \beta_0 \beta_{t-1} \beta_{t-2} \dots \beta_0 \dots = 0.\beta_k \beta_{k-1} \dots \beta_0 (\beta_{t-1} \beta_{t-2} \dots \beta_0)^\infty$$

where $k = 0, 1, \dots, t-1$, cf. Subsection 2.5; or (which is the same) to the numbers $0.(\beta_k \beta_{k-1} \dots \beta_0 \beta_{t-1} \beta_{t-2} \dots \beta_{k+1})^\infty$. That is, all the lines from the limit plot are $y = p^\ell h \bmod 1$, $\ell \in \mathbb{N}_0$, for any line $y = h$ belonging to the limit plot; thus the number of lines in the limit plot does not exceed t . Respectively, being considered as a point set on the torus \mathbb{T}^2 , the limit plot consists of not more than t parallels, cf., e.g., Figures 8 and 9.

Now we present a more formal argument and derive a little bit more information about the number of lines in the limit plot. Given $q \in \mathbb{Z}_p \cap \mathbb{Q}$, represent q as an irreducible fraction $q = a/b$ for suitable $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Note that $p \nmid b$ since $q \in \mathbb{Z}_p$.

Denote

$$\begin{aligned} \mathbf{C}(a/b) = \text{limit points of } \left\{ \left(p^\ell \cdot \left(1 - \frac{a}{b} \right) \right) \bmod 1 : \ell = 0, 1, 2, \dots \right\} = \\ \text{limit points of } \left\{ \left(-p^\ell \cdot \frac{a}{b} \right) \bmod 1 : \ell = 0, 1, 2, \dots \right\}. \end{aligned} \quad (3.30)$$

Since $a/b \in \mathbb{Z}_p \cap \mathbb{Q}$, by Proposition 2.1 a p -adic canonical form of a/b is

$$a/b = \alpha_0 + \alpha_1 p + \dots + \alpha_{r-1} p^{r-1} + (\beta_0 + \beta_1 p + \dots + \beta_{t-1} p^{t-1}) \cdot \sum_{j=0}^{\infty} p^{r+tj} \quad (3.31)$$

for suitable $\alpha_i, \beta_m \in \{0, 1, \dots, p-1\}$, or, in other words, the infinite word that corresponds to a/b is $(\beta_{t-1} \dots \beta_0)^\infty \alpha_{r-1} \dots \alpha_0$. Then from Proposition 2.5 it follows that

$$\begin{aligned} (a/b) \bmod 1 &= (p^r \cdot 0.(\hat{\beta}_{t-1} \dots \hat{\beta}_0)^\infty) \bmod 1 = \\ &= 0.(\hat{\beta}_{t-1-\bar{r}} \hat{\beta}_{t-2-\bar{r}} \dots \hat{\beta}_0 \hat{\beta}_{t-1} \hat{\beta}_{t-2} \dots \hat{\beta}_{t-\bar{r}})^\infty \bmod 1, \end{aligned}$$

where $\hat{\beta}_i = p-1-\beta_i$, $i = 0, 1, 2, \dots, t-1$, and \bar{r} is the least non-negative residue of r modulo t if $t > 1$ or $\bar{r} = 0$ if otherwise. From here in view of (2.6) we deduce that

$$(-a/b) \bmod 1 = 0.(\beta_{t-1-\bar{r}} \beta_{t-2-\bar{r}} \dots \beta_0 \beta_{t-1} \beta_{t-2} \dots \beta_{t-\bar{r}})^\infty \bmod 1$$

and thus

$$\begin{aligned} \mathbf{C}(a/b) &= \\ &= \{0.(\beta_{t-1-\ell} \beta_{t-2-\ell} \dots \beta_0 \beta_{t-1} \beta_{t-2} \dots \beta_{t-\ell})^\infty \bmod 1 : \ell = 0, 1, 2, \dots, t-1\} = \\ &= \left\{ \frac{\text{num}(v)}{p^t - 1} : v \in \{\hat{\zeta}_{t-1} \hat{\zeta}_{t-2} \dots \hat{\zeta}_0, \hat{\zeta}_{t-2} \hat{\zeta}_{t-3} \dots \hat{\zeta}_0 \hat{\zeta}_{t-1}, \hat{\zeta}_{t-3} \hat{\zeta}_{t-4} \dots \hat{\beta}_0 \hat{\zeta}_{t-1} \hat{\zeta}_{t-2}, \dots\} \right\}, \end{aligned}$$

where $(a/b) \bmod 1 = (\zeta_0 + \zeta_1 \cdot p + \dots + \zeta_{t-1} \cdot p^{t-1})(p^t - 1)^{-1}$ (cf. Proposition 2.2 and Corollary 2.7). Now we can suppose that t is a period length of the rational p -adic integer $a/b \in \mathbb{Z}_p \cap \mathbb{Q}$ (cf. Subsection 2.2); then in view of Proposition 2.8 we conclude that

$$\begin{aligned} \mathbf{C}(a/b) &= \{(-p^\ell \cdot (a/b)) \bmod 1 : \ell = 0, 1, \dots, (\text{mult}_b p) - 1\} = \\ &= \{0.(w)^\infty \bmod 1 : w \text{ runs through all cyclic shifts of the word } \beta_{(\text{mult}_b p)-1} \dots \beta_0\} = \\ &= \{0.(v)^\infty \bmod 1 : v \text{ runs through all cyclic shifts of the word } \hat{\zeta}_{(\text{mult}_b p)-1} \dots \hat{\zeta}_0\} = \\ &= \left\{ \left(-p^\ell \cdot \frac{d}{p^{\text{mult}_b p} - 1} \right) \bmod 1 : \ell = 0, 1, \dots, (\text{mult}_b p) - 1 \right\} \end{aligned} \quad (3.32)$$

since

$$\begin{aligned} 1 - \frac{\zeta_0 + \zeta_1 p + \dots + \zeta_{t-1} p^{t-1}}{p^t - 1} &= \frac{\hat{\zeta}_{t-1} + \hat{\zeta}_0 p + \hat{\zeta}_1 p^2 + \dots + \hat{\zeta}_{t-2} p^{t-1}}{p^t - 1} \text{ and} \\ p \cdot \frac{\hat{\zeta}_0 + \hat{\zeta}_1 p + \dots + \hat{\zeta}_{t-1} p^{t-1}}{p^t - 1} &= \hat{\zeta}_{t-1} + \frac{\hat{\zeta}_{t-1} + \hat{\zeta}_0 p + \hat{\zeta}_1 p^2 + \dots + \hat{\zeta}_{t-2} p^{t-1}}{p^t - 1}. \end{aligned}$$

Note that $0.(w)^\infty \bmod 1 = 0.(w)^\infty$ except of the case when $t = 1$ and w is a single-letter word that consists of the only letter $p-1$ (in the latter case $0.(w)^\infty = 1$ and thus $0.(w)^\infty \bmod 1 = 0$). Similarly, $0.(v)^\infty \bmod 1 = 0.(v)^\infty$ except of the case when $a/b \in \mathbb{Z}$ and thus $\zeta_0 = \dots = \zeta_{t-1} = 0$ (so $\hat{\zeta}_0 = \dots = \hat{\zeta}_{t-1} = p-1$ and $0.(v)^\infty = 1$). But this case happens if and only if $a/b \in \mathbb{Z}$; i.e., when $\mathbf{C}(a/b) = \{0\}$.

We now summarize all these considerations in a proposition:

Proposition 3.1. *Let $f_{\mathfrak{A}}: z \mapsto q$ be an automaton function of a finite automaton \mathfrak{A} (therefore $q \in \mathbb{Z}_p \cap \mathbb{Q}$ by Proposition 2.15); then $\mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$ is a disjoint union of t parallels $\mathbf{C}(0, e)$, $e \in \mathbf{C}(q)$, and t is a period length of q (cf. (3.30) and (3.32)).*

Note 3.2. In conditions of Proposition 3.1 the constant $q \in \mathbb{Z}_p \cap \mathbb{Q}$ can be represented as an irreducible fraction $q = a/b$ where $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $p \nmid b$ (we put $b = 1$ and $a = 0$ if $q = 0$). Then the limit plot $\mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$ is a torus link that consists of $t = \text{mult}_b p$ trivial torus cables (parallels) with slopes 0; to the link there corresponds a collection of t complex constants (which are b -th roots of 1)

$$\left\{ \psi_\ell = e^{-2\pi i p^\ell q} : \ell = 0, 1, \dots, (\text{mult}_b p) - 1 \right\},$$

where i stands for imaginary unit $i \in \mathbb{C}$: $i^2 = -1$ (cf. Subsection 2.6).

Being considered in the unit real square \mathbb{I}^2 , the limit plot $\mathbf{LP}(\mathfrak{A})$ is a collection of $t = \text{mult}_b p$ segments of straight lines $y = c(t, k, u)$ that cross \mathbb{I}^2 , where

$$c(t, k, u) = \left(-p^k \cdot \frac{u}{p^t - 1} \right) \bmod 1 = 0.(\hat{\zeta}_{t-1-k} \hat{\zeta}_{t-2-k} \dots \hat{\zeta}_0 \hat{\zeta}_{t-1} \hat{\zeta}_{t-2} \dots \hat{\zeta}_{t-k})^\infty \bmod 1; \quad k = 0, 1, \dots, t-1. \quad (3.33)$$

Here $q \bmod 1 = u(p^t - 1)^{-1}$, $0 \leq u \leq p^t - 2$, and a base p -expansion of u is $u = \zeta_0 + \zeta_1 \cdot p + \dots + \zeta_{t-1} \cdot p^{t-1}$ (cf. Proposition 2.2); $\hat{\zeta} = p - 1 - \zeta$ for $\zeta \in \{0, 1, \dots, p-1\}$. In other words, all the constants $c(t, k, u)$ are of the form

$$c(t, k, u) = 0.v^\infty \bmod 1 = \frac{\text{num}(v)}{p^t - 1} \bmod 1, \quad (3.34)$$

where v runs through all cyclic shifts of the word $\hat{\zeta}_{t-1} \hat{\zeta}_{t-2} \dots \hat{\zeta}_0$; that is, $v \in \{\hat{\zeta}_{t-1} \hat{\zeta}_{t-2} \dots \hat{\zeta}_0, \hat{\zeta}_{t-2} \hat{\zeta}_{t-3} \dots \hat{\zeta}_0 \hat{\zeta}_{t-1}, \dots\}$.

If q is represented in a p -adic canonical form (3.31) rather than in a form of Proposition 2.2, then all the lines of the limit plot can be represented as

$$y = 0.(\beta_{t-1-\ell} \beta_{t-2-\ell} \dots \beta_0 \beta_{t-1} \beta_{t-2} \dots \beta_{t-\ell})^\infty \bmod 1; \quad \ell = 0, 1, 2, \dots, t-1. \quad (3.35)$$

Note that we may omit $\bmod 1$ in (3.34) and in (3.35) in all cases but the case when simultaneously the length t of the period is 1 and $\hat{\zeta}_0 = p - 1$ (respectively, $\beta_0 = p - 1$); but $q \in \mathbb{Z}$ in that case and therefore $\mathbf{C}(q) = \{0\}$.

The following property of the set $\mathbf{C}(q)$ will be used in further proofs:

Corollary 3.3. *Given $q_1, q_2 \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1)$, the following alternative holds: Either $\mathbf{C}(q_1) = \mathbf{C}(q_2)$ or $\mathbf{C}(q_1) \cap \mathbf{C}(q_2) = \emptyset$.*

Proof of Corollary 3.3. The result is clear enough since the numbers that constitute $\mathbf{C}(q)$ are exactly all numbers whose base- p expansions are of the form $0.(u)^\infty$ where u runs through all cyclic shifts of the finite word w which is the (shortest) period of $q \bmod 1$, cf. Note 3.2; nonetheless we give a formal proof which follows.

Given $q_i \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1)$, $i = 1, 2$, represented as irreducible fractions $q_i = a_i/b_i$ whose denominators b_i are co-prime to p , let $\mathbf{C}(q_1) \cap \mathbf{C}(q_2) \neq \emptyset$; then $p^{\ell_1}(a_1/b_1) = p^{\ell_2}(a_2/b_2)$ for suitable $\ell_1, \ell_2 \in \mathbb{N}_0$. If $\ell_1 = \ell_2$ then $a_1/b_1 = a_2/b_2$ and thus $\mathbf{C}(q_1) = \mathbf{C}(q_2)$. Let $\ell_1 > \ell_2$, then $p^{\ell_1 - \ell_2} a_1 b_2 = a_2 b_1$; so since $\gcd(b_1, p) = 1$ we conclude that $a_2 = p^{\ell_1 - \ell_2 + s} a'_2$ for a suitable $s \in \mathbb{N}_0$ and $a'_2 \in \mathbb{Z}$ such that $\gcd(a'_2, p) = 1$. Therefore necessarily $a_1 = p^s a'_1$ where $\gcd(a'_1, p) = 1$ since $\gcd(b_1, p) = \gcd(b_2, p) = 1$. But then we conclude that $p^{\ell_1 - \ell_2 + s} a'_1 b_2 = p^{\ell_1 - \ell_2} a_1 b_2 = a_2 b_1 = p^{\ell_1 - \ell_2 + s} a'_2 b_1$ and therefore $q_1 = p^s q$, $q_2 = p^{\ell_1 - \ell_2 + s} q$ where $q = a'_1/b_1 = a'_2/b_2$. Hence $\mathbf{C}(q_1), \mathbf{C}(q_2) \subset \mathbf{C}(q)$; the inverse inclusion also holds since $\mathbf{C}(p^\ell q) = \mathbf{C}(q)$ for any $q \in \mathbb{Z}_p \cap \mathbb{Q}$ by e.g., (3.35). \square

Example 3.4. Let $p = 2$ and $q = 2/7$. Then $\text{mult}_7 2 = 3$ and the limit plot consists of 3 lines. The binary infinite word that corresponds to the 2-adic canonical representation of $2/7$ is $(011)^\infty 10$, so the period of $2/7$ is 011, the pre-period is 01, and $u = 2 = 0 + 1 \cdot 2 + 0 \cdot 2^2$. Therefore the tree lines of the limit plot are: $y = 0.(101)^\infty = 5/7 = (-2/7) \bmod 1 = c(3, 0, 2)$, $y = 0.(011)^\infty = 6/7 = (-1/7) \bmod 1 = c(3, 2, 2)$, $y = 0.(110)^\infty = 3/7 = (-4/7) \bmod 1 = c(3, 1, 2)$. The limit plot (on the unit square and on the torus) is illustrated by Figures 8 and 9 accordingly.

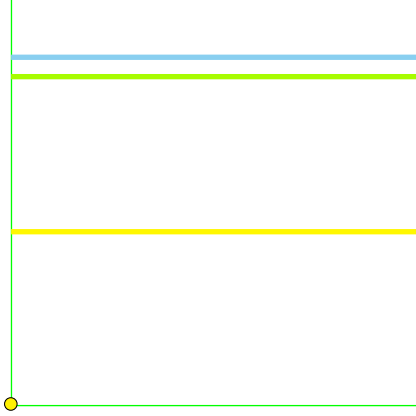


FIGURE 8. A limit plot of the constant function $f(z) = \frac{2}{7}$ ($z \in \mathbb{Z}_2$), in \mathbb{R}^2

FIGURE 9. A limit plot of the same function on the torus \mathbb{T}^2

3.2. Limit plots of linear maps. In this subsection we consider limit plots of linear maps $z \mapsto cz$ ($z \in \mathbb{Z}_p$) which are finite automaton functions. By Proposition 2.15, the latter takes place if and only if $c \in \mathbb{Z}_p \cap \mathbb{Q}$.

Proposition 3.5. *Given $c \in \mathbb{Z}_p \cap \mathbb{Q}$, represent $c = a/b$, where $a \in \mathbb{Z}$, $b \in \mathbb{N}$, a, b are coprime, $p \nmid b$. If \mathfrak{A} is an automaton such that $f_{\mathfrak{A}}(z) = cz$ ($z \in \mathbb{Z}_p$) then $\text{LP}(\mathfrak{A}) = \{(x \bmod 1; (cx) \bmod 1) : x \in \mathbb{R}\} = \mathbf{C}(c, 0)$ is a cable (with a slope c) of the unit 2-dimensional real torus \mathbb{T}^2 . For every $c \in \mathbb{Z}_p \cap \mathbb{Q}$ the automaton \mathfrak{A} may be taken a finite.*

Proof of Proposition 3.5. By Proposition 2.15, the map $z \mapsto cz$ on \mathbb{Z}_p is an automaton function of a finite automaton if and only if $c \in \mathbb{Z}_p \cap \mathbb{Q}$.

Given $x \in [0, 1)$, take $z \in \mathbb{Z}_p$ such that $\lim_{i \rightarrow \infty} z \bmod p^{k_i}/p^{k_i} = x$ for a suitable strictly increasing sequence $k_1, k_2, \dots \in \mathbb{N}$. As $c \in \mathbb{Z}_p \cap \mathbb{Q}$, then $c = u + v/(p^t - 1)$ for suitable $u \in \mathbb{Z}$, $t \in \mathbb{N}$, $v \in \{0, 1, 2, \dots, p^t - 2\}$, by Proposition 2.2. If $t > 1$, then considering residues of k_i modulo t we see that at least one residue (say, $\ell \in \{0, 1, \dots, t-1\}$) occurs in the sequence k_1, k_2, \dots infinitely many times. Therefore $\lim_{j \rightarrow \infty} z \bmod p^{r_j t + \ell}/p^{r_j t + \ell} = x$ for a respective strictly increasing sequence $r_1, r_2, \dots \in \mathbb{N}$. The latter equality trivially holds when $t = 1$: one just takes $r_j = k_j$ and $\ell = 0$. So further we assume that $k_i = r_i t + \ell$, $i = 1, 2, \dots$

For $i = 1, 2, \dots$ we have that

$$\frac{(cz) \bmod p^{k_i}}{p^{k_i}} = \frac{1}{p^{k_i}} ((c \bmod p^{k_i})(z \bmod p^{k_i})) \bmod p^{k_i} = \left(c \bmod p^{k_i} \cdot \frac{z \bmod p^{k_i}}{p^{k_i}} \right) \bmod 1 \quad (3.36)$$

As $0 \leq \ell < t$ and $k_i = r_i t + \ell$, we have that

$$c \bmod p^{k_i} = \left(u + \frac{v}{p^t - 1} \right) \bmod p^{k_i} = \left(u - v \cdot \frac{p^{(r_i+1)t} - 1}{p^t - 1} \right) \bmod p^{k_i} \quad (3.37)$$

Note that the argument of \bmod in the right-hand side of (3.37) is negative once i is sufficiently large; therefore once i is large enough then

$$\left(u - v \cdot \frac{p^{(r_i+1)t} - 1}{p^t - 1} \right) \bmod p^{k_i} = Lp^{k_i} + u - v \cdot \frac{p^{(r_i+1)t} - 1}{p^t - 1}$$

for a suitable $L \in \mathbb{N}$ which does not depend on i (actually it is not difficult to see that $L = \lceil vp^{t-\ell}(p^t - 1)^{-1} \rceil$). Thus,

$$\begin{aligned} \left(c \bmod p^{k_i} \cdot \frac{z \bmod p^{k_i}}{p^{k_i}} \right) \bmod 1 &= \\ &= \left(\left(Lp^{k_i} + u - v \cdot \frac{p^{(r_i+1)t} - 1}{p^t - 1} \right) \cdot \frac{z \bmod p^{k_i}}{p^{k_i}} \right) \bmod 1 = \\ &= \left(L \cdot z \bmod p^{k_i} + u \cdot \frac{z \bmod p^{k_i}}{p^{k_i}} + \frac{v}{p^t - 1} \cdot \frac{z \bmod p^{k_i}}{p^{k_i}} - \frac{vp^{t-\ell}}{p^t - 1} \cdot z \bmod p^{k_i} \right) \bmod 1 = \\ &= \left(c \cdot \frac{z \bmod p^{k_i}}{p^{k_i}} - \frac{vp^{t-\ell}}{p^t - 1} \cdot z \bmod p^{k_i} \right) \bmod 1 \quad (3.38) \end{aligned}$$

Firstly we note that given $w \in \mathbb{N}_0$, $r \in \mathbb{N}$

$$\frac{wp^{rt}}{p^t - 1} \bmod 1 = \left(w \cdot \frac{p^{rt} - 1}{p^t - 1} + \frac{w}{p^t - 1} \right) \bmod 1 = \left(\frac{w}{p^t - 1} \right) \bmod 1 \quad (3.39)$$

as $p^t - 1$ is a factor of $p^{rt} - 1$.

Secondly, put $\bar{z} = p^{t-\ell}z$, then $p^{t-\ell}(z \bmod p^{r_i t + \ell}) = \bar{z} \bmod p^{(r_i+1)t}$ and

$$x = \lim_{i \rightarrow \infty} \frac{z \bmod p^{k_i}}{p^{k_i}} = \lim_{i \rightarrow \infty} \frac{\bar{z} \bmod p^{r_i t}}{p^{r_i t}},$$

so in (3.38)

$$\frac{vp^{t-\ell}}{p^t - 1} \cdot z \bmod p^{r_i t + \ell} = \frac{v}{p^t - 1} \cdot \bar{z} \bmod p^{(r_i+1)t}$$

and $\bar{z} = zp^{t-\ell} \in \mathbb{Z}_p$ (recall that $k_i = r_i t + \ell$ where $\ell \in \{0, 1, \dots, t-1\}$).

Let $\bar{z} = \zeta_0 + \zeta_1 p^t + \zeta_2 p^{2t} + \dots$ be a base- p^t representation of \bar{z} (that is, $\zeta_j \in \{0, 1, \dots, p^t - 1\}$); then by combining (3.36) and (3.38) with (3.39) we get

$$\begin{aligned} \frac{(cz) \bmod p^{k_i}}{p^{k_i}} &= \left(c \cdot \frac{z \bmod p^{k_i}}{p^{k_i}} - \frac{v}{p^t - 1} \cdot \text{wt}_{p^t}(\bar{z} \bmod p^{(r_i+1)t}) \right) \bmod 1 = \\ &= \left(c \cdot \frac{z \bmod p^{k_i}}{p^{k_i}} - \frac{v}{p^t - 1} \cdot (\text{wt}_{p^t}(\bar{z} \bmod p^{(r_i+1)t})) \bmod (p^t - 1) \right) \bmod 1 \quad (3.40) \end{aligned}$$

where wt_{p^t} stands for a p^t -weight of a natural number, that is, the sum of digits of the number in its base- p^t representation; i.e., $\text{wt}_{p^t}(\bar{z} \bmod p^{(r_i+1)t}) = \zeta_0 + \zeta_1 + \dots + \zeta_i \in \mathbb{N}_0$. Therefore every limit point of the sequence $((cz) \bmod p^{k_i} / p^{k_i})_{i=1}^\infty$ is of the form

$$\left(cx + \frac{vw}{p^t - 1} \right) \bmod 1 \quad (3.41)$$

for a suitable $w \in \{0, 1, \dots, p^t - 2\}$.

We claim that, on the other hand, given $x \in [0, 1)$ and $h \in \{0, v, 2v \bmod (p^t - 1), \dots, ((p^t - 2)v) \bmod (p^t - 1)\}$ (that is, h lying in the ideal $\langle v \rangle$ of the residue ring $\mathbb{Z}/(p^t - 1)\mathbb{Z}$ generated by v) there exists $z \in \mathbb{Z}_p$ and a strictly increasing sequence $k_1, k_2, \dots \in \mathbb{N}$ such that

$$x = \lim_{i \rightarrow \infty} \frac{z \bmod p^{k_i}}{p^{k_i}}, \text{ and}$$

$$\frac{(cz) \bmod p^{k_i}}{p^{k_i}} = \left(c \cdot \frac{z \bmod p^{k_i}}{p^{k_i}} + \frac{h}{p^t - 1} \right) \bmod 1.$$

Indeed, take $z \in \mathbb{Z}_p$ and $k_i = r_i t + \ell$ as above; then all limit points of the sequence $((cz) \bmod p^{k_i} / p^{k_i})_{i=1}^\infty$ are of the form (3.41) for, say, $w = w_1, \dots, w_s \in \{0, 1, \dots, p^t - 2\}$. If $h \equiv vw_j \pmod{(p^t - 1)}$ for some $j = 1, 2, \dots, s$, then there is nothing to prove; if $h \not\equiv vw_j \pmod{(p^t - 1)}$ for all $j = 1, 2, \dots, s$ then we tweak z as follows. As the point of the form (3.41) for $w = w_1$ is a limit point of the sequence $((cz) \bmod p^{k_i} / p^{k_i})_{i=1}^\infty$ then $(-vw_1) \bmod (p^t - 1)$ occurs in the sequence $((-v((\mathbf{wt}_{p^t} \bar{z}) \bmod p^{(r_i+1)t})) \bmod (p^t - 1))_{i=1}^\infty$ infinitely many times (cf. (3.40)); so some $\bar{w} \in \{0, 1, \dots, p^t - 2\}$ such that $v\bar{w} \equiv vw_1 \pmod{(p^t - 1)}$ occurs in the sequence $((\mathbf{wt}_{p^t} \bar{z}) \bmod p^{(r_i+1)t}) \bmod (p^t - 1)$ infinitely many times:

$$\bar{w} = ((\mathbf{wt}_{p^t} \bar{z}) \bmod p^{(r_i+1)t}) \bmod (p^t - 1) = (\zeta_0 + \zeta_1 + \dots + \zeta_i) \bmod (p^t - 1)$$

for $i = i_1, i_2, \dots$ ($1 < i_1 < i_2 < \dots$).

As $h \in \langle v \rangle$, then $h \equiv -v\bar{w} \pmod{(p^t - 1)}$ for a suitable $\tilde{w} \in \{0, 1, \dots, p^t - 2\}$. Now put $\tilde{z} = \zeta_0 + \tilde{\zeta}_1 p^t + \zeta_2 p^{2t} + \zeta_3 p^{3t} + \dots$, where $\tilde{\zeta}_1 \equiv \zeta_1 - \bar{w} + \tilde{w} \pmod{(p^t - 1)}$; then $\tilde{w} = (\mathbf{wt}_{p^t} \tilde{z}) \bmod p^{(r_i+1)t} \bmod (p^t - 1)$. But $\lim_{i \rightarrow \infty} (z \bmod p^{k_i} / p^{k_i}) = \lim_{i \rightarrow \infty} (\tilde{z} \bmod p^{k_i} / p^{k_i}) = x$; so finally we conclude by (3.40) that

$$\lim_{j \rightarrow \infty} \frac{(c\tilde{z}) \bmod p^{r_{i_j} t + \ell}}{p^{r_{i_j} t + \ell}} = \left(cx + \frac{h}{p^t - 1} \right) \bmod 1.$$

Thus we have shown that

$$\mathbf{LP}(\mathfrak{A}) = \left\{ \left(x; \left(cx + \frac{e}{p^t - 1} \right) \bmod 1 \right) : x \in [0, 1), e \in \langle v \rangle \right\}. \quad (3.42)$$

But the right-hand side in (3.42) is a cable of torus with slope c since

$$\left\{ \left(x; \left(cx + \frac{h}{p^t - 1} \right) \bmod 1 \right) : x \in [0, 1), h \in \langle v \rangle \right\} = \{(y \bmod 1; (cy) \bmod 1) : y \in \mathbb{R}\}. \quad (3.43)$$

Indeed, if $y_1 = y + n$ for some $n \in \mathbb{Z}$ then $y_1 \bmod 1 = y \bmod 1$ and $(cy_1) \bmod 1 = (c(y + n)) \bmod 1 = (((u + v(p^t - 1)^{-1})(y + n)) \bmod 1 = (cy + vn(p^t - 1)^{-1}) \bmod 1 = (cy + ((vn) \bmod (p^t - 1)) \cdot (p^t - 1)^{-1}) \bmod 1$, and (3.43) follows. This concludes the proof. \square

Example 3.6. Take $p = 2$ and $c = 5/3$. Figures 6 and 7 illustrate the limit plot of the function $f(z) = (5/3) \cdot z$ in \mathbb{I}^2 and in \mathbb{T}^2 respectively.

3.3. Limit plots of affine maps. In this subsection we combine the above two cases (constant maps and linear maps) into a single one to describe limit plots of finite automata whose functions are affine, i.e., of the form $z \mapsto c \cdot z + q$ ($z \in \mathbb{Z}_p$). It is evident that the limit plot should be a torus link consisting of several disjoint cables with slopes c since the limit plot of the constant q is a collection of parallels, cf. Propositions 3.5 and 3.1. We will give a formal proof of this claim and find the number of knots in the link.

Recall that by Proposition 2.15 the map $z \mapsto c \cdot z + q$ of \mathbb{Z}_p into itself is an automaton function of some finite automaton if and only if $c, q \in \mathbb{Z}_p \cap \mathbb{Q}$. The

following proposition shows that we do not alter the limit plot of the map once we replace q by $q + n$ for arbitrary $n \in \mathbb{Z}$.

Proposition 3.7. *Given $f: z \mapsto cz + q$ ($z \in \mathbb{Z}_p$) where $c, q \in \mathbb{Z}_p \cap \mathbb{Q}$, denote $\bar{q} = q \bmod 1$, $\bar{f}: z \mapsto cz + \bar{q}$. Then $\mathbf{LP}(f) = \mathbf{LP}(\bar{f})$.*

Proof of Proposition 3.7. Indeed, once $n \in \mathbb{Z}$ then $\lim_{k \rightarrow \infty} n \bmod p^k/p^k \in \{0, 1\}$; the limit is 1 if and only if n is negative since given a canonical p -adic representation $n = \alpha_0 + \alpha_1 p + \dots$ of a negative $n \in \mathbb{Z}$, all $\alpha_i = p - 1$ if i is large enough, cf. Subsection 2.2. Therefore $(\lim_{k \rightarrow \infty} (z + n) \bmod p^k/p^k) \bmod 1 = (\lim_{k \rightarrow \infty} (z \bmod p^k + n \bmod p^k) \bmod p^k/p^k) \bmod 1 = \lim_{k \rightarrow \infty} (z \bmod p^k/p^k + n \bmod p^k/p^k) \bmod 1 = (\lim_{k \rightarrow \infty} z \bmod p^k/p^k) \bmod 1$ for all $z \in \mathbb{Z}$. \square

Note that the map $z \mapsto cz + \bar{q}$ from the statement of Proposition 3.7 is an automaton function for a suitable finite automaton \mathfrak{B} and $\mathbf{LP}(\mathfrak{A}) = \mathbf{LP}(\mathfrak{B})$, where \mathfrak{A} is a finite automaton whose automaton function is f .

Now we describe limit plot of a special affine map with $c = 1, q \neq 0$.

Lemma 3.8. *Given a finite automaton \mathfrak{A} whose automaton function is $f(z) = z + q$ ($q \in \mathbb{Z}_p \cap \mathbb{Q}$ then), the limit plot $\mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$ is a link of a finite number of torus knots which are cables $\mathbf{C}(1, e)$ where e is running over $\mathbf{C}(q)$.*

Proof of Lemma 3.8. We will prove that once \mathfrak{A} is a finite automaton such that $f_{\mathfrak{A}}(z) = f(z) = z + q$ then

$$\mathbf{LP}(\mathfrak{A}) = \bigcup_{e \in \mathbf{C}(q)} \mathbf{C}(1, e). \quad (3.44)$$

Note that if $e = 0$ and $e \in \mathbf{C}(q)$ then $\mathbf{C}(q) = \{0\}$ by Proposition 3.1 and there is nothing to prove. So further we assume that $e \in \mathbf{C}(q)$ and $e \neq 0$.

By Proposition 3.7 we may assume that $q \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, -1)$ then $q = d \cdot (p^t - 1)^{-1} - 1$ for suitable $d \in \{0, 1, \dots, p^t - 2\}$, cf. Proposition 2.2; that is, $d = \zeta_{t-1} + \zeta_{t-2}p + \dots + \zeta_0 p^{t-1}$, where $\zeta_0, \dots, \zeta_{t-1} \in \{0, 1, \dots, p-1\}$ and therefore

$$\begin{aligned} q &= -(\zeta_{t-1} + \zeta_{t-2}p + \dots + \zeta_0 p^{t-1})(1 + p^t + p^{2t} + \dots) - 1 = \\ &((p-1 - \zeta_{t-1}) + (p-1 - \zeta_{t-2})p + \dots + (p-1 - \zeta_0)p^{t-1})(1 + p^t + p^{2t} + \dots) \end{aligned}$$

as $(p^t - 1)^{-1} = -(1 + p^t + p^{2t} + \dots)$ in \mathbb{Z}_p by Note 2.3. Therefore, in \mathbb{Z}_p the rational number q can be represented as

$$q = (\eta_0 + \eta_1 p + \dots + \eta_{t-1} p^{t-1}) \cdot (1 + p^t + p^{2t} + \dots), \quad (3.45)$$

where $\eta_j = p - 1 - \zeta_{t-1-j}$, $j = 0, 1, \dots, t-1$.

Given $x \in [0, 1)$ take a sequence $n_i \in \mathbb{N}_0$, $i = 1, 2, \dots$, and a strictly increasing sequence $k_i \in \mathbb{N}$, $i = 1, 2, \dots$, such that $k_i \geq \lfloor \log_p n_i \rfloor + 1$, $\lim_{i \rightarrow \infty} n_i/p^{k_i} = x$, and $k_i \bmod t = s \in \{0, 1, \dots, t-1\}$ for all $i = 1, 2, \dots$. This is always possible since if, e.g., $x = \xi_1 p^{-1} + \xi_2 p^{-2} + \dots$ for suitable $\xi_1, \xi_2, \dots \in \{0, 1, \dots, p-1\}$ then one takes $n_i = \xi_1 p^{j-1} + \xi_2 p^{j-2} + \dots + \xi_{j-1}$ where $j = it + s$ and put $k_i = it + s$ for $i = 1, 2, \dots$.

Considering a sequence $(n_i + q)_{i=0}^\infty$ in \mathbb{Z}_p , we see that

$$\frac{(n_i + q) \bmod p^{k_i}}{p^{k_i}} = \left(\frac{n_i}{p^{k_i}} + \frac{q \bmod p^{k_i}}{p^{k_i}} \right) \bmod 1 \quad (3.46)$$

But $k_i = it + s$, $s \in \{0, 1, \dots, t-1\}$; thus

$$\begin{aligned} \left(\lim_{i \rightarrow \infty} \left(\frac{q \bmod p^{k_i}}{p^{k_i}} \right) \right) \bmod 1 &= \left(\lim_{i \rightarrow \infty} ((\eta_0 + \eta_1 p + \dots + \eta_{s-1} p^{s-1}) p^{-s} + \right. \\ &\quad (\eta_0 + \eta_1 p + \dots + \eta_{t-1} p^{t-1}) \cdot (p^{-it-s} + p^{(-i+1)t-s} + \dots + p^{-t-s})) \bmod 1 = \\ &\quad \left. 0.(\eta_{s-1} \eta_{s-2} \dots \eta_0 \eta_{t-1} \eta_{t-2} \dots \eta_s)^\infty \bmod 1 \right) \quad (3.47) \end{aligned}$$

if $s \neq 0$, or

$$\begin{aligned} \left(\lim_{i \rightarrow \infty} \left(\frac{q \bmod p^{k_i}}{p^{k_i}} \right) \right) \bmod 1 &= \\ \left(\lim_{i \rightarrow \infty} ((\eta_0 + \eta_1 p + \dots + \eta_{t-1} p^{t-1}) \cdot (p^{-it} + p^{(-i+1)t} + \dots + p^{-t})) \bmod 1 &= \\ 0.(\eta_{t-1} \eta_{t-2} \dots \eta_0)^\infty \bmod 1 \right) \quad (3.48) \end{aligned}$$

if $s = 0$. From (3.48) and (3.47) it follows that $\lim_{i \rightarrow \infty} (q \bmod p^{k_i} / p^{k_i}) \bmod 1 \in \mathbf{C}(q)$ by (3.33) of Note 3.2. Thus we have proved that given $x \in [0, 1)$ and $e \in \mathbf{C}(q)$, necessarily $(x, (x + e) \bmod 1) \in \mathbf{LP}(\mathfrak{A})$; so $\mathbf{LP}(\mathfrak{A}) \supset \mathbf{C}(1, e)$ for every $e \in \mathbf{C}(b)$.

On the other hand, given $z \in \mathbb{Z}_p$ and a strictly increasing sequence $k_1, k_2, \dots \in \mathbb{N}$, by combining (3.48) and (3.47) with (3.33) of Note 3.2 we conclude that all limit points of the sequence $q \bmod p^{k_i} / p^{k_i}$, $i = 1, 2, \dots$, are in $\mathbf{C}(q)$ by an argument similar to the above one. Therefore, limit points of the sequence $(z \bmod p^{k_i} / p^{k_i} + q \bmod p^{k_i} / p^{k_i}) \bmod 1$, $i = 1, 2, \dots$, are all of the form $(x + e) \bmod 1$, where x is an limit point of the sequence $z \bmod p^{k_i} / p^{k_i}$ and $e \in \mathbf{C}(q)$. This proves that $\mathbf{LP}(\mathfrak{A}) \subset \cup_{e \in \mathbf{C}(q)} \mathbf{C}(1, e)$ and that (3.44) is true. \square

Now we are ready to prove the main claim of the Section.

Theorem 3.9. *Given $c, q \in \mathbb{Z}_p$, a map $z \mapsto cz + q$ of \mathbb{Z}_p into itself is an automaton function of a finite automaton if and only if $c, q \in \mathbb{Z}_p \cap \mathbb{Q}$. Given a finite automaton \mathfrak{A} whose automaton function is $f(z) = cz + q$ for $c, q \in \mathbb{Z}_p \cap \mathbb{Q}$, represent c, q as irreducible fractions $c = a/b$, $q = a'/b'$, where $a, a' \in \mathbb{Z}$, $b, b' \in \mathbb{N}$ and $\gcd(a, b) = \gcd(a', b') = \gcd(b, p) = \gcd(b', p) = 1$; then the limit plot $\mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$ is a link of $\text{mult}_m p$ torus knots, where $m = b' / \gcd(b, b')$, and every knot of the link is a cable $\mathbf{C}(c, e)$ for $e \in \mathbf{C}(q)$:*

$$\mathbf{LP}(\mathfrak{A}) = \{(y \bmod 1; (cy + e) \bmod 1) : y \in \mathbb{R}, e \in \mathbf{C}(q)\}. \quad (3.49)$$

Moreover, $\mathbf{C}(c, e_1) = \mathbf{C}(c, e_2)$ for $e_1, e_2 \in \mathbf{C}(q)$ if and only if $r_1 \equiv r_2 \pmod{m}$ where $e_i = (-p^{r_i} q) \bmod 1$, $i = 1, 2$, cf. (3.33).

Note 3.10. Once $m = 1$, i.e., once $b' \mid b$, the congruence $r_1 \equiv r_2 \pmod{m}$ holds trivially, $\text{mult}_1 p = 1$ and the link consists of a single knot; so in that case $\mathbf{C}(c, e_1) = \mathbf{C}(c, e_2)$ for all $e_1, e_2 \in \mathbf{C}(q)$.

Proof of Theorem 3.9. The first statement of the theorem is already proved, see Proposition 2.15.

Given $q, c \in \mathbb{Z}_p \cap \mathbb{Q}$, we have that

$$c = u + \frac{v}{p^t - 1}, \quad (3.50)$$

$$q = \frac{w}{p^T - 1} \quad (3.51)$$

for suitable $u \in \mathbb{Z}$, $t, T \in \mathbb{N}$, $v \in \{0, 1, 2, \dots, p^t - 2\}$, $w \in \{0, 1, \dots, p^T - 2\}$, by Proposition 2.2. Note that we may assume that $0 < q < 1$ since the set of all limit points of the sequence $((z + q) \bmod p^k / p^k)_{k=1}^\infty$ is the same as that of the sequence

$((z + q \bmod 1) \bmod p^k/p^k)_{k=1}^\infty$ by Proposition 3.7 and the case $q = 0$ is already considered, cf. Proposition 3.5.

Now we will prove that $\mathbf{LP}(\mathfrak{A}) \supset \mathbf{C}(c, e)$ for $e \in \mathbf{C}(q)$. As $q \in \mathbb{Z}_p \cap \mathbb{Q} \cap (0, 1)$, the canonical p -adic representation of q is eventually periodic and the period length of q is T , cf. Subsection 2.2. Now fix $e \in \mathbf{C}(q)$, take corresponding $d \in \{0, 1, \dots, T-1\}$ and consider a sequence $n_j = d + iT \in \mathbb{N}$ ($j = 1, 2, \dots$); then $\lim_{j \rightarrow \infty} q \bmod p^{n_j}/p^{n_j} = e$, cf. the proof of Lemma 3.8. Given $x \in [0, 1)$ take $z \in \mathbb{Z}_p$ and a sequence $\mathcal{K} = (k_i = \ell + r_i t)_{i=1}^\infty$ as in the proof of Proposition 3.5; so $x = \lim_{i \rightarrow \infty} z \bmod p^{k_i}/p^{k_i}$. Note that if $\bar{z} = p^m z$ for some $m \in \mathbb{N}_0$ then $x = \lim_{i \rightarrow \infty} \bar{z} \bmod p^{k_i+m}/p^{k_i+m}$; so the proof of Proposition 3.5 remains valid if one substitutes \bar{z} for z and any strictly increasing subsequence (\bar{k}_i) of the sequence $\mathcal{K} = (k_i = m + \ell + r_i t)$ for the sequence \mathcal{K} .

We claim that for some $m \in \mathbb{N}_0$ there exist an increasing sequence $j_s \in \mathbb{N}$ and a subsequence $(\bar{r}_s)_{s=1}^\infty$ of the sequence $(r_i)_{i=1}^\infty$ such that

$$m + \ell + \bar{r}_s t = d + j_s T \text{ for all } s = 1, 2, 3, \dots \quad (3.52)$$

Indeed, let $D = \gcd(T, t)$ be the greatest common divisor of T and t ; then $T = \tilde{T}D$, $t = \tilde{t}D$, \tilde{t} and \tilde{T} are co-prime. As the infinite sequence $(r_i)_{i=1}^\infty$ is strictly increasing, there exists $\tilde{n} \in \{0, 1, \dots, \tilde{t}-1\}$ such that $r_i + \tilde{n} \equiv 0 \pmod{\tilde{T}}$ for infinitely many $i \in \mathbb{N}$, say, for $i = i_1, i_2, \dots$. Put $\bar{r}_s = r_{i_s}$; $s = 1, 2, 3, \dots$

Take the smallest $\bar{n} = \tilde{n} + n\tilde{T}$, $n \in \mathbb{N}_0$, such that $d - \ell + \bar{n}\tilde{T}D \geq 0$, then put $m = d - \ell + \bar{n}\tilde{T}D$ and find j_s from the equation (3.52) which now is equivalent to the equation $(\bar{n} + \bar{r}_s)\tilde{t} = j_s\tilde{T}$: As $\bar{n} + \bar{r}_s = h_s\tilde{T}$ for a suitable $s \in \mathbb{N}$ by the definition of \bar{n} , one sees that $j_s = \tilde{t}h_s$ for $s = 1, 2, 3, \dots$ thus proving our claim.

We conclude now that given arbitrary $y \in \mathbb{R}$ and $e \in \mathbf{C}(q)$ there exist $\bar{z} \in \mathbb{Z}_p$ and a sequence $\check{\mathcal{K}} = (\check{k}_s = \bar{r}_s t + \ell + m = d + j_s T)$ such that

$$y \bmod 1 = x = \lim_{s \rightarrow \infty} \frac{\bar{z} \bmod p^{\check{k}_s}}{p^{\check{k}_s}}, \quad (3.53)$$

$$(cy) \bmod 1 = \lim_{s \rightarrow \infty} \frac{(c\bar{z}) \bmod p^{\check{k}_s}}{p^{\check{k}_s}}, \quad (3.54)$$

$$e = \lim_{s \rightarrow \infty} \frac{q \bmod p^{\check{k}_s}}{p^{\check{k}_s}}; \quad (3.55)$$

cf. (3.42), (3.43) and Proposition 3.1. Therefore, $\lim_{s \rightarrow \infty} (c\bar{z} + q) \bmod p^{\check{k}_s}/p^{\check{k}_s} = \lim_{s \rightarrow \infty} ((c\bar{z}) \bmod p^{\check{k}_s}/p^{\check{k}_s} + q \bmod p^{\check{k}_s}/p^{\check{k}_s}) \bmod 1 = (cy + e) \bmod 1$ and so the point $(y \bmod 1, (cy + e) \bmod 1) \in \mathbf{C}(c, e)$ is in $\mathbf{LP}(\mathfrak{A})$. Thus we have proved that $\mathbf{LP}(\mathfrak{A}) \supset \mathbf{C}(c, e)$ for every $e \in \mathbf{C}(q)$.

On the other hand, given arbitrary $z \in \mathbb{Z}_p$ and arbitrary strictly increasing sequence $k_1, k_2, \dots \in \mathbb{N}$, limit points of the point sequence $(z \bmod p^{k_i}/p^{k_i}; (cz) \bmod p^{k_i}/p^{k_i})$ are all in $\mathbf{C}(c, 0)$ by Proposition 3.5 whereas limit points of the sequence $q \bmod p^{k_i}/p^{k_i}$ are all in $\mathbf{C}(q)$ by Proposition 3.1. Therefore limit points of the point sequence $((z \bmod p^{k_i}/p^{k_i}; (cz + q) \bmod p^{k_i}/p^{k_i}))_{i=1}^\infty = ((z \bmod p^{k_i}/p^{k_i}, ((cz) \bmod p^{k_i}/p^{k_i} + q \bmod p^{k_i}/p^{k_i}) \bmod 1))_{i=1}^\infty$ are all in $\cup_{e \in \mathbf{C}(q)} \mathbf{C}(c, e)$. Finally we conclude that $\mathbf{LP}(\mathfrak{A}) = \cup_{e \in \mathbf{C}(q)} \mathbf{C}(c, e)$; or (which is the same) that

$$\mathbf{LP}(\mathfrak{A}) = \{(y \bmod 1; (cy + e) \bmod 1) : y \in \mathbb{R}, e \in \mathbf{C}(q)\} \quad (3.56)$$

Note that it may happen that $\mathbf{C}(c, q) = \mathbf{C}(c, q_1)$ even if $q \neq q_1$ (and even $q \notin \mathbf{C}(q_1)$): For instance, (3.42) shows that $\mathbf{C}(c, q) = \mathbf{C}(c, 0)$ for some $q \neq 0$. Therefore to finish the proof we must now calculate the number of pairwise distinct cables $\mathbf{C}(c, e)$ when $e \in \mathbf{C}(q)$.

During the proof of Proposition 3.5 we have shown that (in the notation of the proposition under the proof)

$$\{(y \bmod 1; (cy) \bmod 1) : y \in \mathbb{R}\} = \left\{ \left(y \bmod 1; \left(cy + \frac{j}{b} \right) \bmod 1 \right) : y \in \mathbb{R} \right\}$$

for every $j \in \mathbb{Z}$, cf. equation (3.43) and the text which follows it. Therefore $\mathbf{C}(c, e_1) = \mathbf{C}(c, e_2)$ if $e_1 - e_2 \equiv (j/b) \bmod 1$ for some $j \in \mathbb{Z}$. The converse statement is also true: if $\mathbf{C}(c, e_1) = \mathbf{C}(c, e_2)$ then $e_1 - e_2 \equiv (j/b) \bmod 1$ for some $j \in \mathbb{Z}$.

To prove this, for $h \in \mathbf{C}(q)$ let $A(c, h)$ be a set of all points where the cable $\mathbf{C}(c, h)$ crosses zero meridian of the torus \mathbb{T}^2 ; that is,

$$A(c, h) = \mathbf{AP} \left(\left\{ \left(0; \left(\frac{(cz) \bmod p^{s_r}}{p^{s_r}} + h \right) \bmod 1 \right) : z \in \mathbb{Z}_p, \lim_{r \rightarrow \infty} \frac{z \bmod p^{s_r}}{p^{s_r}} = 0 \right\} \right),$$

where $s_1, s_2, \dots \in \mathbb{N}$, $s_1 < s_2 < \dots$; therefore by (3.41)

$$\mathbf{AP} \left(\left(\left(\frac{(cz) \bmod p^{s_r}}{p^{s_r}} + h \right) \bmod 1 \right)_{r=0}^{\infty} \right) = \left\{ \left(\frac{j}{b} + h \right) \bmod 1 : j = 0, 1, 2, \dots \right\}. \quad (3.57)$$

Finally, as $\mathbf{C}(c, e_1) = \mathbf{C}(c, e_2)$ if and only if $A(c, e_1) = A(c, e_2)$ since the both cables cross zero meridian at a same angle (which is equal to $\arctan c$), this means that $\mathbf{C}(c, e_1) = \mathbf{C}(c, e_2)$ if and only if $e_1 - e_2 \equiv jb^{-1} \pmod{1}$ for some $j \in \mathbb{N}_0$, as claimed.

Now we are able to calculate the number of torus knots (cables) which constitutes the link $\mathbf{LP}(\mathfrak{A})$. Let for some $j_1, j_2 \in \{0, 1, \dots, b-1\}$, ($j_1 \neq j_2$) and $e_1, e_2 \in \mathbf{C}(q)$ the following equality holds:

$$\left(\frac{j_1}{b} + e_1 \right) \bmod 1 = \left(\frac{j_2}{b} + e_2 \right) \bmod 1. \quad (3.58)$$

We see that $e_i = -p^{r_i} \left(\frac{a'}{b'} \right) \bmod 1$ for suitable $r_i \in \{0, 1, \dots, (\text{mult}_{b'} p) - 1\}$ by Note 3.2 ($i = 1, 2$). Therefore (3.58) is equivalent to the congruence

$$p^{r_1} \frac{a'}{b'} - p^{r_2} \frac{a'}{b'} \equiv \frac{j}{b} \pmod{1}$$

for a suitable $j \in \{0, 1, \dots, b-1\}$; but the latter congruence in turn is equivalent to the congruence

$$p^{r_2} (p^{r_1-r_2} - 1) a' n \equiv jm \pmod{nm d}, \quad (3.59)$$

where $d = \gcd(b', b)$, $m = b'/d$, $n = b/d$ (we assume that $r_1 > r_2$ since the case $r_1 = r_2$ is trivial). From here it follows that $p^{r_2} (p^{r_1-r_2} - 1) a' n \equiv 0 \pmod{m}$ once $m \neq 1$; therefore necessarily $r_1 \equiv r_2 \pmod{\text{mult}_m p}$ since $\gcd(b', b) = \gcd(p, b) = \gcd(p, b') = 1$. So $(p^{r_1-r_2} - 1) = mh$ for a suitable $h \in \mathbb{N}$ and thus (3.59) is equivalent to the congruence $p^{r_2} h a' n \equiv j \pmod{nd}$, and the latter congruence gives the value of j (modulo $b = nd$) so that (3.58) is satisfied. This means that when $m \neq 1$, 3.58 holds if and only if $r_1 \equiv r_2 \pmod{\text{mult}_m p}$. Thus, if $m \neq 1$ (that is, if b' is not a factor of b) then the number of pairwise distinct torus knots in the link is $\text{mult}_m p$.

In the remaining case when $m = 1$ (i.e., when b' divides b) (3.59) always holds: If $p^{r_1-r_2} \equiv 1 \pmod{d}$ then we can take $j = 0$ to satisfy (3.59); otherwise the left-hand side of (3.59) just gives an expression for a unique residue j modulo $b = nd$ (which thus satisfies (3.59)). Therefore the link consist of a unique cable; so the number of pairwise distinct cables in the link is $1 = \text{mult}_1 p$ in this case as well. This concludes the proof. \square

Note 3.11. In conditions of Theorem 3.9 note that $b'|b$ is the only case when the link $\mathbf{LP}(\mathfrak{A})$ consists of a single cable. Note also that from the proof of Theorem 3.9 it is clear that if the number $\#\mathbf{C}(q)$ of points in $\mathbf{C}(q)$ is 1 then the link necessarily consists of a single cable. By note 3.2, $\#\mathbf{C}(q) = 1$ if and only if the period length of q is 1 and therefore $q \bmod 1 = 0.(\xi)^\infty \bmod 1$ for some $\xi \in \{0, 1, \dots, p-1\}$.

Example 3.12. Let $p = 2$ and $f(z) = (3/5) \cdot z + (1/3)$. Then in conditions of Theorem 3.9 we have that $m = 3$ and therefore the link consists of $\text{mult}_3 2 = 2$ cables with slopes $3/5$, cf. Figures 10 and 11.

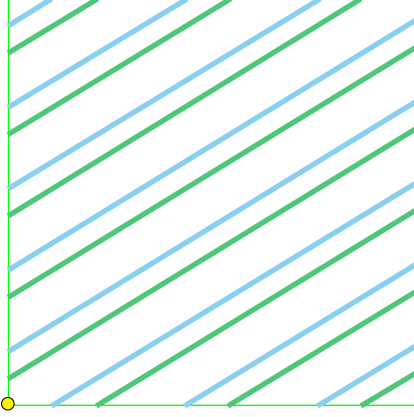


FIGURE 10. Limit plot of the function $f(z) = \frac{3}{5}z + \frac{1}{3}$, $z \in \mathbb{Z}_2$, in \mathbb{R}^2

FIGURE 11. Limit plot of the same function on the torus \mathbb{T}^2

Corollary 3.13. *There is a one-to-one correspondence between maps of the form $f: z \mapsto \frac{a}{b}z + \frac{a'}{b'}$ on \mathbb{Z}_p (where $\frac{a}{b}, \frac{a'}{b'} \in \mathbb{Z}_p \cap \mathbb{Q}$; $a, a' \in \mathbb{Z}$; $b, b' \in \mathbb{N}$) and collections of $\text{mult}_m p$ complex-valued exponential functions $\psi_k: \mathbb{R} \rightarrow \mathbb{C}$ of real variable $y \in \mathbb{R}$*

$$\left\{ \psi_k(y) = e^{i(\frac{a}{b}y - 2\pi p^k \frac{a'}{b'})} : k = 0, 1, 2, \dots, (\text{mult}_m p) - 1 \right\}.$$

Here $i \in \mathbb{C}$ is imaginary unit and $m = b' / \gcd(b, b')$.

Proof of Corollary 3.13. Indeed, embedding the unit torus \mathbb{T}^2 into a 3-dimensional Euclidean space \mathbb{R}^3 and using cylindrical coordinates as in Note 2.27, in view of Theorem 3.9 every knot from the link can be expressed in the form (2.29) with $\omega = 2\pi e$ for $e \in \mathbf{C}(q)$ since $\cos \omega$ and $\sin \omega$ specifies position of the point where the knot crosses zero meridian of the torus (i.e., when $\theta \equiv 0 \pmod{2\pi}$ in (2.29)). But $q = a'/b'$ and thus $\mathbf{C}(q) = \{(-p^\ell \cdot (a'/b')) \bmod 1 : \ell = 0, 1, \dots, (\text{mult}_{b'} p) - 1\}$ by (3.32). As two such knots (with accordingly $\omega_i = 2\pi e_i$, $i = 1, 2$) coincide if and only if $\omega_1 \equiv \omega_2 \pmod{2\pi \cdot (a/b)}$ by (2.29), i.e., if and only if $e_1 \equiv e_2 \pmod{a/b}$. But the latter congruence is equivalent to (3.58); so finally the assertion follows from Theorem 3.9. \square

4. FINITE COMPUTABILITY

In this section we introduce central notion of the paper, the *finite computability*, and prove some technical results which will be needed further during the proof of main result of the paper, the affinity of finitely computable smooth functions, cf. further Section 5.

Definition 4.1. A non-empty point set $S \subset \mathbb{I}^2$ ($S \subset \mathbb{T}^2$, $S \subset \mathbb{I} \times \mathbb{S}$, $S \subset \mathbb{S} \times \mathbb{I}$) is called (*ultimately*) *finitely computable* (or, (*ultimately*) *computable by a finite automaton*) if there exists a finite automaton \mathfrak{A} such that S is a subset of $\mathbf{P}(\mathfrak{A})$ (of $\mathbf{LP}(\mathfrak{A})$). We say that the automaton \mathfrak{A} (*ultimately*) *computes* the set S ; and \mathfrak{A} is called an (*ultimate*) *computing automaton* of the set S .

In most further cases given a real function $g: D \rightarrow \mathbb{R}$ with the domain $D \subset \mathbb{R}$ by the *graph of the function* (on the torus \mathbb{T}^2) we mean the point subset $\mathbf{G}_D(g) = \{(x \bmod 1; g(x) \bmod 1) : x \in D\} \subset \mathbb{T}^2$. However, given a function $g: D \rightarrow T$ where either $D \subset [0, 1]$ or $D \subset \mathbb{S}$ and T is either $[0, 1]$ or \mathbb{S} , we call a graph \mathbf{G}_D of the function g the set $\{(\bar{x}; \overline{g(x)}) : x \in D\}$ where either $\bar{x} = x$ if $D \subset [0, 1]$ or $\bar{x} = x \bmod 1$ if $D \subset \mathbb{S}$ and accordingly either $\overline{g(x)} = g(x)$ if $T = [0, 1]$ or $\overline{g(x)} = (g(x)) \bmod 1$ if $T = \mathbb{S}$. In the sequel we always explain what is meant by $\mathbf{G}_D(g)$ if this is not clear from the context. Also, we may omit the subscript D when it is clear what is the domain.

Definition 4.2. Given a real function $g: D \rightarrow \mathbb{R}$ with domain $D \subset \mathbb{R}$ and an automaton \mathfrak{A} , the function g is called (*ultimately*) *computable by \mathfrak{A} at the point $x \in D$* if $(x \bmod 1; g(x) \bmod 1) \in \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^2$ ($(x \bmod 1; g(x) \bmod 1) \in \mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$). Also, if either $D \subset [0, 1]$ or $D \subset \mathbb{S}$ and $g: D \rightarrow T$ where either $T = [0, 1]$ or $T = \mathbb{S}$ we will say that \mathfrak{A} (*ultimately*) *computes g at the point $x \in D$* if $(\bar{x}; \overline{g(x)}) \in \mathbf{LP}(\mathfrak{A})$ where either $\bar{x} = x$ if $D \subset [0, 1]$ or $\bar{x} = x \bmod 1$ if $D \subset \mathbb{S}$ and accordingly either $\overline{g(x)} = g(x)$ if $T = [0, 1]$ or $\overline{g(x)} = (g(x)) \bmod 1$ if $T = \mathbb{S}$ (cf. Note 2.17).

Given a real function $g: D \rightarrow \mathbb{R}$ with domain $D \subset \mathbb{R}$, the function g is called (*ultimately*) *finitely computable* (or, (*ultimately*) *computable by a finite automaton*) if there exists a finite automaton \mathfrak{A} such that $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^2$ ($\mathbf{G}(g) \subset \mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$). The automaton \mathfrak{A} which (*ultimately*) *computes* the function g is called the (*ultimate*) *computing automaton* of the function g . In a similar manner we define these notions for the cases when $g: D \rightarrow T$ and D, T are as above.

4.1. The mark-ups. In loose terms, when assigning a real-valued function $f^{\mathfrak{A}}: [0, 1] \rightarrow [0, 1]$ to automaton \mathfrak{A} via Monna map $\text{mon}: \mathbb{Z}_p \rightarrow \mathbb{R}$ (cf. subsection 2.5) one feeds the automaton by a base- p -expansion of argument $x \in [0, 1]$ and considers the output as a base- p expansion of $f^{\mathfrak{A}}(x)$: A base- p expansion specifies a unique right-infinite word in the alphabet \mathbb{F}_p and the automaton ‘reads the word from head to tail’, i.e., is feeded by digits of the base- p expansion from left to right (i.e., digits on more significant positions are feeded prior to digits on less significant positions); and the output word specifies a base- p expansion of a unique real number from $[0, 1]$.

To examine functions computed by automata in the meaning of Definition 4.2 it would also be convenient to work with base- p expansions of real numbers; but the problem is that we need feed the automaton by a right-infinite word in the inverse order ‘from tail (which is at infinity) to head’: Digits on less significant positions (the rightmost ones) should be feeded prior to digits on more significant positions (the leftmost ones). So straightforward inversion is impossible since it is unclear which letter should be the first when feeding the automaton this way; thus output word is undefined and so is the real number whose base- p expansion is the output word. In this subsection we rigorously specify this inversion and develop some techniques needed in further proofs.

Let a function $g: D \rightarrow \mathbb{S}$ (or $g: D \rightarrow [0, 1]$) whose domain D is either a subset of a real unit circle \mathbb{S} or a subset of a unit segment $[0, 1]$ be ultimately computable by a finite automaton $\mathfrak{A} = \mathfrak{A}(s_0)$; that is, for any $x \in D$ there exists $x \in \mathbb{Z}_p$ such that x is a limit point of the sequence $(z \bmod p^k / p^k)_{k=1}^{\infty}$ and $g(x)$ is a limit point of the sequence $((f_{\mathfrak{A}}(z)) \bmod p^k / p^k)_{k=1}^{\infty}$, where $f_{\mathfrak{A}}: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is automaton function

of the automaton \mathfrak{A} , cf. Definition 4.2 and Definition 2.16. As said, further to examine finitely computable real functions it is however more convenient to work with automata maps as maps of reals into reals rather than to consider automata functions on p -adic integers and then represent $x \in \mathbb{R}$ and $g(x) \in \mathbb{R}$ as limit points of the sequences $(z \bmod p^k/p^k)_{k=1}^\infty$ and $((f_{\mathfrak{A}}(z)) \bmod p^k/p^k)_{k=1}^\infty$, respectively.

Further in this subsection we are going to show that once $x \in D$ and once $x = 0.\chi_1\chi_2\dots$ is a base- p expansion of x , we can find a state $s = s(x) \in \mathcal{S}$ of the automaton \mathfrak{A} and a strictly increasing infinite sequence of indices $1 \leq k_1 < k_2 < \dots$ such that the sequence $(0.\mathfrak{a}_s(\chi_1\chi_2\dots\chi_{k_j}))_{j=1}^\infty$ tends to $(g(x)) \bmod 1$ (recall that $\mathfrak{a}_s(\zeta_1\zeta_2\dots\zeta_\ell)$ is an ℓ -letter output word of the automaton $\mathfrak{A}(s)$ whose initial state is s once the automaton has been feeded by the ℓ -letter input word $\zeta_1\zeta_2\dots\zeta_\ell$, cf. Subsection 2.3). This means, loosely speaking, that once we feed the automaton $\mathfrak{A}(s)$ with approximations $0.\chi_1\chi_2\dots\chi_{k_j}$ of x , the automaton outputs the sequence of approximations $0.\mathfrak{a}_s(\chi_1\chi_2\dots\chi_{k_j})$ of $g(x)$, and these sequences tend to x and to $g(x)$ accordingly while $j \rightarrow \infty$. Moreover, we will show that if the function g is continuous then there exists a state $s \in \mathcal{S}$ such that all $x \in D$ for which $s(x) = s$ constitute a dense subset in D .

Recall that given $x \in (0, 1)$, there exists a (right-)infinite word $w = \gamma_0\gamma_1\dots$ over $\{0, 1, \dots, p-1\}$ such that

$$x = 0.\gamma_0\gamma_1\dots = 0.w = \sum_{i=0}^{\infty} \gamma_i p^{-i-1}, \quad (4.60)$$

the *base- p expansion* of x . If x is not of the form $x = n/p^k$ for some $n = \alpha_0 + \alpha_1 p + \dots + \alpha_\ell p^\ell \in \{0, 1, \dots, p^k - 1\}$, where $\ell = \mathbf{le}(n) = \lfloor \log_p n \rfloor + 1$ is the length of the base- p expansion of $n \in \mathbb{N}_0$ (recall that we put $\lfloor \log_p 0 \rfloor = 0$, cf. Subsection 2.4), $\alpha_0, \alpha_1, \dots, \alpha_\ell \in \{0, 1, \dots, p-1\}$, then the right-infinite word $\mathbf{wrd}(x) = \gamma_0\gamma_1\dots$ over $\{0, 1, \dots, p-1\}$ is uniquely defined (and the corresponding x is said to have a *unique base- p expansion*); else there are exactly two infinite words,

$$\mathbf{wrd}^r(x) = \alpha_0\alpha_1\dots\alpha_{\ell-1}\alpha_\ell 00\dots = \alpha_0\alpha_1\dots\alpha_{\ell-1}\alpha_\ell(0)^\infty \quad (4.61)$$

$$\mathbf{wrd}^l(x) = \alpha_0\alpha_1\dots\alpha_{\ell-1}(\alpha_\ell - 1)(p-1)(p-1)\dots = \alpha_0\alpha_1\dots\alpha_{\ell-1}(\alpha_\ell - 1)(p-1)^\infty, \quad (4.62)$$

where $\alpha_\ell \neq 0$, such that $x = 0.\mathbf{wrd}^r(x) = 0.\mathbf{wrd}^l(x)$. In that case x is said to have a *non-unique base- p expansion*; the corresponding base- p expansions are called *right* and *left* respectively. Both 0 and 1 are assumed to have unique base- p expansions since $0 = 0.00\dots$, $1 = 0.(p-1)(p-1)\dots$; so $\mathbf{wrd}(0) = 00\dots$, $\mathbf{wrd}(1) = (p-1)(p-1)\dots$. This way we define $\mathbf{wrd}(x)$ for all $x \in [0, 1]$; and to $x = n/p^k$ we will usually put into the correspondence both infinite words $\mathbf{wrd}^l(x)$ and $\mathbf{wrd}^r(x)$ if converse is not stated explicitly. The only difference in considering a unit circle \mathbb{S} rather than the unit segment $\mathbb{I} = [0, 1]$ is that we identify 0 and 1 and thus have two representations for 0, $0.(0)^\infty$ and $0 = 1 \bmod 1 = 0.(p-1)^\infty$.

Given a finite word $w = \alpha_{m-1}\alpha_{m-2}\dots\alpha_0$, we denote via \vec{w} the (right-)infinite word $\vec{w} = \alpha_{m-1}\alpha_{m-2}\dots\alpha_0(0)^\infty$ and we put $0.\vec{w} = 0.\alpha_{m-1}\alpha_{m-2}\dots\alpha_0(0)^\infty\dots$ (note that then $0.\vec{w} = \rho(w)$). Of course, $0.\vec{w} = 0.w = \sum_{i=0}^{m-1} \alpha_i p^{-m+i}$; but we use notation $0.\vec{w}$ if we want to stress that we deal with infinite base- p expansion. To unify our notation, we also may write $\vec{w} = \zeta_1\zeta_2\dots$ for a (right-)infinite word $w = \zeta_1\zeta_2\dots$; then $0.\vec{w} = 0.w = 0.\zeta_1\zeta_2\dots$.

Let $\vec{w} = \gamma_0\gamma_1\dots$ be a (right-)infinite word over $\mathbb{F}_p = \{0, 1, \dots, p-1\}$. Given an automaton \mathfrak{A} with the initial state s , we further denote via $\mathfrak{a}_s(\vec{w})$ the set of all limit points of the sequence $(\rho(\mathfrak{a}_s(\gamma_0\gamma_1\dots\gamma_k)))_{k=0}^\infty$. We may omit the subscript s if it is clear from the context what is the initial state of the automaton.

Given $x \in [0, 1]$ further $\mathbf{a}_s(x)$ stands for $\mathbf{a}_s(\vec{w}(x))$ if x admits a unique base- p expansion, and $\mathbf{a}_s(x) = \mathbf{a}_s(\vec{w}(x)_l) \cup \mathbf{a}_s(\vec{w}(x)_r)$ if the expansion is non-unique (thus, if x admits both left and right base- p expansions). We also consider $\mathbf{a}_s(x)$ for $x \in \mathbb{S}$ rather than for $x \in [0, 1]$; in that case we take for 0 both base- p expansions $0.(0)^\infty$ and $0.(p-1)^\infty$ (since $0 = (0.(p-1)^\infty) \bmod 1$) and reduce modulo 1 all limit points of all sequences $(\rho(\mathbf{a}_s(\gamma_0\gamma_1 \dots \gamma_k)))_{k=0}^\infty$. We further use the same symbol $\mathbf{a}_s(x)$ independently of whether we consider $x \in [0, 1]$ or $x \in \mathbb{S}$; we make special remarks when this may cause a confusion.

We stress that $\mathbf{a}_s(w)$ is a uniquely defined finite word whenever $w \in \mathcal{W}$ is a finite word (and therefore $\rho(\mathbf{a}_s(w))$ consists of a single number), but in the case when w is an infinite word or w is a real number from $[0, 1]$ (or $w \in \mathbb{S}$), the set $\mathbf{a}_s(w)$ may contain more than one element.

Given $x \in \mathbb{Q} \cap [0, 1]$, in view of Lemma 2.10 it is clear that if the automaton \mathfrak{A} is finite then $\mathbf{a}(x) \in \mathbb{Q} \cap [0, 1]$ since a real number is rational if and only if its base- p expansion is eventually periodic. The following proposition reveals some more details about $\mathbf{a}(x)$ for a rational x ; and especially for $x = 0$.

Proposition 4.3. *If \mathfrak{A} is finite, $x \in \mathbb{Q} \cap [0, 1]$ then $\mathbf{a}(x) \subset \mathbb{Q} \cap [0, 1]$ and $\mathbf{a}(x)$ is a finite set. Moreover, if $x \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1]$ then $\mathbf{a}(x) \subset \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1]$. In particular, if $x = 0 \in \mathbb{S}$ then $\mathbf{a}(x) = \mathbf{C}(q_1) \cup \mathbf{C}(q_2)$ for suitable $q_1, q_2 \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1]$ (cf. Subsection 3.1). Let a \mathfrak{A} -computable function $g: D \rightarrow \mathbb{S}$ be defined on the domain $D \subset \mathbb{S}$ and continuous at $0 \in D$. If the domain D is open then there exists $q \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1]$ such that $\mathbf{a}(0.(0)^\infty) = \mathbf{a}(0.(p-1)^\infty) \in \mathbf{C}(q)$; and either $\mathbf{a}(0.(0)^\infty) \in \mathbf{C}(q)$ or $\mathbf{a}(0.(p-1)^\infty) \in \mathbf{C}(q)$ if the domain D is half-open and x is a boundary of D .*

Proof of Proposition 4.3. Follows from Lemma 2.10 and Proposition 3.1 (see the proof of the latter).

Given $x \in \mathbb{Q} \cap [0, 1]$, a base- p expansion of x is eventually periodic, cf. (2.5): $x = 0.\chi_0 \dots \chi_{k-1}(\xi_0 \dots \xi_{n-1})^\infty$. Given x , take n, k the smallest possible (note that then the word $v = \chi_0 \dots \chi_{k-1}$ may be empty). From the definition of $\mathbf{a}(x)$ it follows that $\mathbf{a}(x)$ consists of all limit points of the sequences $\mathcal{K}(r) = (\rho((v(u)^k r)))_{k=K}^\infty$, where K is large enough and $r \in \{\xi_0, \xi_0 \xi_1, \dots, \xi_0 \xi_1 \dots \xi_{n-1}\}$ are all suffixes of the word $u = \xi_0 \dots \xi_{n-1}$, for every right-infinite word w which corresponds to a base- p expansion of $x = 0.w$. As the automaton $\mathfrak{A} = \mathfrak{A}(s_0)$ is finite, the number of states it reaches after being fed by either of words r , where is finite; say, these states are $s_1, \dots, s_N \in \mathbb{S}$. By the same reason, being fed by the words $(u)^K$ where K is large enough, the automata $\mathfrak{A}_1 = \mathfrak{A}(s_1), \dots, \mathfrak{A}_N = \mathfrak{A}(s_N)$ output respectively words $v_1(u_1)^{K_1} t_1, \dots, v_N(u_N)^{K_N} t_N$, where the words $u_1, \dots, u_N, t_1, \dots, t_N$ do not depend on K , each of the words v_1, \dots, v_N is either empty or a prefix of the respective word w_1, \dots, w_N , and all the output words $v_1(u_1)^{K_1} t_1, \dots, v_N(u_N)^{K_N} t_N$ have the same length as the one of the input word $(u)^K$, cf. Lemma 2.10. That is, the output words of automata \mathfrak{A}_i are all of the form $(\bar{u})^L t$, where \bar{u} stands for a cyclically shifted word u , and after outputting the word $(\bar{u})^L t$, each automaton \mathfrak{A}_i , $i = 1, 2, \dots, N$, reaches some of finitely many its states, say, $s'_{i1}, \dots, s'_{iM(i)}$. After reaching respective state, the automaton is fed by the word v and outputs the corresponding output word $v'_{i,j}$, $j = 1, 2, \dots, M(i)$. Therefore, all limit points of the sequences $\mathcal{K}(r)$ are of the form $0.v'_{i,j}(\bar{u}_i)^\infty$ where \bar{u}_i runs through a (sub)set of all cyclic shifts of the word u_i , $i = 1, 2, \dots, N$, $j = 1, 2, \dots, M(i)$. But there are only finite number of points of that form; therefore, given a base- p expansion of $x = 0.\vec{w}$, the set $\mathbf{a}(0.\vec{w})$ is a union of a finite number points of the said form. As every $x \in \mathbb{Q}$ has at most two base- p expansions, this proves the first claim of the proposition.

If $x \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1]$, then base- p expansion of x is purely periodic by Proposition 2.5: $x = 0.(\chi_0 \dots \chi_{n-1})^\infty$. Therefore once the automaton \mathfrak{A} is being fed by finite

words of the form $w^L t$, where $w = \chi_0 \dots \chi_{n-1}$, t is a suffix of w or empty and L is large enough, by Lemma 2.10 the corresponding output word will be of the form $(u_t)^{N(t)} v_t$, and the number of different words u_t is finite since the number of different words t is finite. Applying the same argument as above we conclude that all limit points of corresponding sequences are of the form $0.(u)^\infty$ where u runs through a finite number of finite words. But by Corollary 2.6, all these points are in $\mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1]$. This proves the second claim of the proposition.

To prove the final claim, we must consider both base- p representations of zero point of the unit circle \mathbb{S} : $0 = 0.(0)^\infty$ and $0 = 0.(p-1)^\infty$. Sending a left-infinite zero sequence to the automaton \mathcal{A} , the output sequence will be of the form $w^\infty t$ by suitable finite words w, t by Lemma 2.10; so $\mathfrak{a}(0^\infty)$ consists of all points of the form $0.(u)^\infty$, where u runs through all cyclic shifts of the word $w = \chi_{n-1} \dots \chi_0$; therefore $\mathfrak{a}(0^\infty) = \mathbf{C}(q_1)$ for a suitable $q_1 \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1)$, cf. Note 3.2. By the same reason, $\mathfrak{a}((p-1)^\infty) = \mathbf{C}(q_2)$ for a suitable $q_2 \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1)$. In the case when the \mathfrak{A} -computable function $g: D \rightarrow \mathbb{S}$ is continuous at 0 and there exists an open neighborhood U of 0 such that $U \subset D$ then necessarily $g(0) \in \mathfrak{a}(0.0^\infty)$ and $g(0) \in \mathfrak{a}(0.(p-1)^\infty)$; so $\mathbf{C}(q_1) \cap \mathbf{C}(q_2) \neq \emptyset$ and therefore $\mathbf{C}(q_1) = \mathbf{C}(q_2)$ by Corollary 3.3. If no such neighborhood U exists then the domain is half-open and 0 is a boundary point; thus due to the continuity of g at 0 we see that either $g(0) \in \mathfrak{a}(0.0^\infty)$ or $g(0) \in \mathfrak{a}(0.(p-1)^\infty)$ and the conclusion follows. \square

Corollary 4.4. *Let \mathfrak{A} be a finite automaton, let $(x; y) \in \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^2$, and let $x \in \mathbb{Z}_p \cap \mathbb{Q} \setminus \{0\}$; then $y \in \mathbb{Z}_p \cap \mathbb{Q}$. If $x = 0$ then $y \in [0, 1) \cap \mathbb{Q}$; moreover, there exists $y \in \mathbb{Z}_p \cap \mathbb{Q}$ such that $(0; y) \in \mathbf{P}(\mathfrak{A})$.*

Proof of Corollary 4.4. As $x \in \mathbb{Z}_p \cap \mathbb{Q}$ and $x \in [0, 1)$ then by Corollary 2.7 the base- p expansion is purely periodic; that is, $x = 0.w$, where $w \in \mathcal{W}^\infty$ is a right-infinite periodic word: $w = (v)^\infty$ for a suitable finite non-empty word $v \in \mathcal{W}$. As $(x, y) \in \mathbf{P}(\mathfrak{A})$ then by Note 2.18 there exists a sequence $(u_i)_{i=0}^\infty$ of finite non-empty words such that $\lim_{i \rightarrow \infty} 0.u_i = x$ and simultaneously $\lim_{i \rightarrow \infty} 0.\mathfrak{a}(u_i) = y$. Let $x \neq 0$; then v is not a 1-letter zero word: $v \neq 0$. Therefore since $\lim_{i \rightarrow \infty} 0.u_i = x$, for all sufficiently large i the words u_i must be of the form $u_i = (v)^{L_i} \bar{u}_i$ where L_i increases unboundedly while $i \rightarrow \infty$. Therefore we may assume that the sequence L_i is strictly increasing (we consider a strictly increasing subsequence of the sequence (L_i) if otherwise) and that all u_i are of the form $u_i = (v)^{L_i} \bar{u}_i$. Let $s(i)$ be a state the automaton \mathfrak{A} reaches after being feeded by the word \bar{u}_i ($s(i) = s_0$ if $\bar{u}_i = \phi$ is empty). As the automaton \mathfrak{A} is finite, then there are only finitely many pairwise distinct $s(i)$, say these are $s'(1), \dots, s'(n)$. Now we consider automata $\mathfrak{A}(s'(1)), \dots, \mathfrak{A}(s'(n))$ and apply the same argument as in the proof of the second statement of Proposition 4.3 thus proving that $y \in \mathbb{Z}_p \cap \mathbb{Q}$. The same argument can be applied for the case when $x = 0$ but there exists an infinite sequence of words u_i whose lengths are increasing unboundedly while $i \rightarrow \infty$. Therefore the only rest case is now $x = 0$ and once the word sequence $(u_i)_{i=0}^\infty$ is such that $\lim_{i \rightarrow \infty} 0.u_i = x$ and lengths of u_i are bounded; $\Lambda(u_i) \leq K$ for all $i \in \mathbb{N}_0$. But this just means that for all sufficiently large i all the words u_i are K -letter zero words: $u_i = (0)^K$ for a suitable $K \in \mathbb{N}$. But then $y = 0.\mathfrak{a}((0)^K)$; thus $y \in [0, 1) \cap \mathbb{Q}$. The last claim of the corollary trivially follows from Proposition 4.3 since once $y \in \mathfrak{a}(0)$ then $(0; y) \in \mathbf{P}(\mathfrak{A})$ by the definition of $\mathbf{P}(\mathfrak{A})$. \square

The following definition introduces an important technical notion, the mark-up, which will be used in further proofs:

Definition 4.5. Given a function $g: D \rightarrow [0, 1]$ defined on the domain $D \subset [0, 1]$, an automaton \mathfrak{A} , and a point $x \in D$ consider a right-infinite word w such that $x =$

$0.w$, cf. (4.60), (4.61), (4.62). An infinite strictly increasing sequence i_0, i_1, i_2, \dots over \mathbb{N}_0 is called an *s-mark-up of the* (right-infinite) *word* $w = \gamma_0\gamma_1\dots$ w.r.t. g and \mathfrak{A} (or briefly a *mark-up* when it is clear what g , \mathfrak{A} and s are meant) if there exists a state $s \in \mathcal{S}$ of the automaton \mathfrak{A} such that $\lim_{k \rightarrow \infty} \rho(\mathfrak{a}_s(\gamma_0\gamma_1\dots\gamma_{i_k})) = g(x)$.

Remark. Given $x \in D \subset \mathbb{S}$, the mark-ups of x are defined exactly in the same way. Note only that the point $x = 0$ of \mathbb{S} coincides with the point $x = 1$ and $1 = 0 = 0.000\dots = 0.(p-1)(p-1)(p-1)\dots \in \mathbb{S}$ as $\mathbb{S} = \mathbb{R} \bmod 1$. In a similar way we define the mark-up when $g: D \rightarrow \mathbb{S}$.

The following proposition shows, speaking loosely, that if a continuous real function is finitely computable, then all base- p expansions of all its arguments can be marked-up:

Proposition 4.6. *Given a continuous function $g: (a, b) \rightarrow [0, 1]$ (or, which makes no difference, $g: (a, b) \rightarrow \mathbb{S}$ where $(a, b) \subset \mathbb{S}$ is an arc of the unit circle \mathbb{S}) let $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$ for a suitable finite automaton \mathfrak{A} . Then for every $x \in (a, b)$ and every infinite word w such that $x = 0.w$ there exists an s-mark-up, for a suitable state $s = s(w) \in \mathcal{S}$ of the automaton \mathfrak{A} .*

Proof of Proposition 4.6. The idea of the proof is as follows: Once feeding a finite automaton \mathfrak{A} by infinite sequence of finite words $\gamma_0, \gamma_0\gamma_1, \gamma_0\gamma_1\gamma_2, \dots$ over \mathbb{Z}_p , the automaton reaches some of its states infinitely many times; this state s specifies a mark-up ($i(s)$) since corresponding sequences of approximations $0.\gamma_0\dots\gamma_{i(s)}$ and $\mathfrak{a}_s(0.\gamma_0\dots\gamma_{i(s)})$ tend accordingly to $x = 0.\gamma_0\gamma_1\gamma_2\dots$ and to $g(x)$ due to the continuity of g at x . Now we prove the proposition rigorously.

Firstly consider the case when $x \in (a, b)$ has a unique base- p expansion, say, $x = 0.\gamma_0\gamma_1\dots = 0.w$, where $w = \gamma_0\gamma_1\dots$. As $g(x)$ is \mathfrak{A} -computable, there exists a sequence $w_0, w_1, w_2, \dots \in \mathcal{W}$ of finite non-empty words such that $\rho(w_0), \rho(w_1), \rho(w_2), \dots \in (a, b)$, $\lim_{i \rightarrow \infty} \rho(w_i) = x$ and $\lim_{j \rightarrow \infty} \rho(\mathfrak{a}(w_i)) = g(x)$. Note that the sequence $(\Lambda(w_i))_{i=0}^\infty$ is increasing since otherwise $x = n/p^r$ for suitable $n, r \in \mathbb{N}_0$ as $\lim_{i \rightarrow \infty} \rho(w_i) = x$ and thus x has a non-unique base- p expansion. We may assume that $(\Lambda(w_i))_{i=0}^\infty$ is a strictly increasing sequence since otherwise we just take a suitable subsequence of $(w_i)_{i=0}^\infty$. Moreover, by the same reason we may assume that $\Lambda(w_i) > i$.

Consider a word sequence $\bar{w}_0 = \gamma_0, \bar{w}_1 = \gamma_0\gamma_1, \bar{w}_2 = \gamma_0\gamma_1\gamma_2, \dots$. As $x \in (a, b)$, there exists $N \in \mathbb{N}_0$ such that $0.\bar{w}_i \in (a, b)$ once $i \geq N$. Without loss of generality we may assume that $N = 1$. As $\lim_{i \rightarrow \infty} 0.w_i = 0.\gamma_0\gamma_1\dots = x$, for every $n \in \mathbb{N}_0$ there exists $M(n) \in \mathbb{N}_0$, $M(n) \geq n$, such that $|0.w_i - 0.\bar{w}_j| < p^{-n}$ provided $i, j \geq M(n)$; therefore as $\Lambda(w_i) > i \geq M(n) \geq n$, we conclude that $w_i = \gamma_0\dots\gamma_n v_i$ for $i \geq M(n)$ and suitable finite word v_i . Given $n \in \mathbb{N}_0$, let $M(n)$ be the smallest with the said property; this way we obtain an increasing sequence $M(0) < M(1) < M(2) < \dots$. Considering the subsequence $(w_{M(j)})_{j=0}^\infty$ of the word sequence $(w_i)_{i=0}^\infty$, we see that $w_{M(j)} = \gamma_0\dots\gamma_j r_j$ for $j = 0, 1, 2, \dots$ and suitable finite non-empty words r_j , that $\lim_{j \rightarrow \infty} \rho(w_{M(j)}) = x$ and that $\lim_{j \rightarrow \infty} \rho(\mathfrak{a}(w_{M(j)})) = g(x)$. Now to the word sequence $(r_j)_{j=0}^\infty$ we put into the correspondence the sequence $(s(r_j))_{j=0}^\infty$ of states of the automaton \mathfrak{A} , where $s(r_j)$ is the state the automaton \mathfrak{A} reaches after being fed by the input word r_j . As the number of different states of \mathfrak{A} is finite, in the sequence $(s(r_j))_{j=0}^\infty$ at least one state, say s , occurs in the sequence $(s(r_j))_{j=0}^\infty$ infinitely many times; say, for $j = j_0, j_1, j_2, \dots$ ($j_0 < j_1 < j_2 < \dots$). Therefore

$$\lim_{k \rightarrow \infty} \rho(\gamma_0\dots\gamma_{j_k}) = 0.\gamma_0\gamma_1\dots = x \quad (4.63)$$

$$\lim_{k \rightarrow \infty} \rho(\mathfrak{a}_s(\gamma_0\dots\gamma_{j_k})) = \lim_{k \rightarrow \infty} \rho(\mathfrak{a}(w_{M(j_k)})) = g(x) \quad (4.64)$$

Recall that $\mathfrak{a} = \mathfrak{a}_{s_0}$ where s_0 is the initial state of the automaton $\mathfrak{A} = \mathfrak{A}(s_0)$. Note that nowhere in the argument above we have used that g is continuous.

Now consider the case when $x = n/p^r$ for suitable $n, r \in \mathbb{N}_0$, $n \in \{0, 1, \dots, p^r - 1\}$. In this case, let $0.\gamma_0\gamma_1\dots$ be either of base- p expansions $\text{wrd}^r(x)$, $\text{wrd}^l(x)$. We will show that similarly to the case when a base- p expansion is unique, in the case under consideration there also exist $s \in \mathcal{S}$ and sequences $i_0 < i_1 < i_2 < \dots$, $M(i_0) < M(i_1) < M(i_2) < \dots$ over \mathbb{N}_0 such that $M(i_k) \geq i_k$ for all $k \in \mathbb{N}_0$ and both (4.63) and (4.64) hold.

For this purpose, consider arbitrary sequence w_0, w_1, w_2, \dots of right-infinite words over $\{0, 1, \dots, p-1\}$ which are not eventually periodic and such that $\gamma_0\dots\gamma_i$ is a prefix of w_i for all $i = 0, 1, 2, \dots$. Then $\lim_{i \rightarrow \infty} 0.w_i = x$ and therefore all $0.w_i \in (a, b)$ once $i \geq I$ where I is large enough (we may assume that $I = 0$; otherwise we consider a subsequence $(w_i)_{i=I}^\infty$ rather than the whole sequence $(w_i)_{i=0}^\infty$). Note that then $\lim_{i \rightarrow \infty} g(0.w_i) = g(x)$ as g is continuous on (a, b) ; therefore there exists a sequence $(S(i))_{i=0}^\infty$ over \mathbb{N} such that for all $i = 0, 1, 2, \dots$ the following inequality holds:

$$|g(0.w_i) - g(x)| < p^{-S(i)} \quad (4.65)$$

Moreover, we may assume that the sequence $(S(i))_{i=0}^\infty$ is strictly increasing (if not, we consider a corresponding infinite subsequence of the sequence $(w_i)_{i=0}^\infty$ rather than the whole sequence).

Consider now a word $w_i = \gamma_{i0}\gamma_{i1}\dots$ from the above word sequence (note that $\gamma_{i\ell} = \gamma_\ell$ for $\ell = 1, 2, \dots, i$). As every $0.w_i$ is a unique base- p expansion of the corresponding real number from (a, b) , there exists a state $s(i)$ of the automaton \mathfrak{A} and a strictly increasing sequence $\mathcal{J}(s(i)) = (j_{ik})_{k=0}^\infty$ of numbers from \mathbb{N}_0 such that

$$\lim_{k \rightarrow \infty} \rho(\mathfrak{a}_{s(i)}(\gamma_{i0}\gamma_{i1}\dots\gamma_{ij_{ik}})) = g(0.w_i), \quad (4.66)$$

cf. the case we just have considered above at the beginning of the proof of the proposition. Therefore, for any $k \in \mathbb{N}_0$ there exists $K(j_{ik}) \in \mathbb{N}$ such that

$$|\rho(\mathfrak{a}_{s(i)}(\gamma_{i0}\gamma_{i1}\dots\gamma_{ij_{ik}})) - g(0.w_i)| < p^{-K(j_{ik})}, \quad (4.67)$$

and there exists a strictly increasing sequence of k such that the corresponding sequence of $K(j_{ik})$ is also strictly increasing in force of (4.66). Without loss of generality we may assume that the sequence $(K(j_{ik}))_{k=0}^\infty$ is strictly increasing (otherwise we consider a corresponding subsequence of the sequence $\mathcal{J}(s(i))$).

As a total number of states of \mathfrak{A} is finite, in the infinite sequence $(s(i))_{i=0}^\infty$ at least one state, say s , occurs infinitely many times. We may assume that $s(i) = s$ for all $i \in \mathbb{N}_0$; otherwise we just consider respective subsequence of $(w_i)_{i=0}^\infty$ rather than the whole sequence. As the sequence $(j_{ik})_{k=0}^\infty$ is strictly increasing, all $j_{ik} > i$ once k is large enough. Given $i \in \mathbb{N}_0$, denote via $N(i) \in \mathbb{N}$ the smallest number such that $j_{ik} > i$ once $k \geq N(i)$. We again may assume that $N(i) = 0$; if otherwise we will just consider the subsequence $(j_{ik})_{k=N(i)}^\infty$ rather than the whole sequence $(j_{ik})_{k=0}^\infty$. Then $\gamma_{i0}\gamma_{i1}\dots\gamma_{ij_{ik}} = \gamma_0\dots\gamma_{ir_{ik}}$ for all k where r_{ik} is a non-empty finite word.

Let $s'(i, k) \in \mathcal{S}$ be a state the automaton $\mathfrak{A}(s)$ reaches after being feeded by the input word r_{ik} (the latter state s is defined above). As the total number of states of $\mathfrak{A}(s)$ is finite, in the sequence $(s'(i, k))_{k=0}^\infty$ at least one state, say $s'(i)$, occurs infinitely many times. Moreover, by the same reason at least one state, say s' , occurs in the sequence $(s'(i))_{i=0}^\infty$ infinitely many times. And again, without loss of generality we may assume that $s'(i, k) = s'$ for all i, k ; otherwise we consider corresponding subsequences of the sequences $(w_i)_{i=0}^\infty$ and $(j_{ik})_{k=0}^\infty$. Note that being feeded by the input word $\gamma_{i0}\gamma_{i1}\dots\gamma_{ij_{ik}} = \gamma_0\dots\gamma_{ir_{ik}}$, the automaton $\mathfrak{A}(s)$ (rightmost letters are feeded prior to leftmost ones), the automaton outputs a word of length $j_{ik} + 1$ whose

(left) suffix of length $i + 1$ is the word which outputs the automaton $\mathfrak{A}' = \mathfrak{A}(s')$ if being feeded by the word $\gamma_0 \dots \gamma_i$. Therefore

$$|\rho(\mathfrak{a}'(\gamma_0 \dots \gamma_i)) - \rho(\mathfrak{a}_s(\gamma_{i0}\gamma_{i1} \dots \gamma_{ij_{ik}}))| < p^{-i+1} \quad (4.68)$$

Now combining (4.65), (4.67) and (4.68) we conclude that $\lim_{i \rightarrow \infty} \rho(\mathfrak{a}'(\gamma_0 \dots \gamma_i)) = g(x)$; but $\lim_{i \rightarrow \infty} \rho(\gamma_0 \dots \gamma_i) = x$ since $0.\gamma_0\gamma_1 \dots$ is a base- p expansion of x . This finally proves the proposition. \square

Note 4.7. Actually during the proof of Proposition 4.6 we have shown that the following claim is true: *Let the function $g: U \rightarrow \mathbb{S}$ (or, $g: U \rightarrow \mathbb{I}$) be defined on an open neighbourhood $U \subset \mathbb{S}$ (or, $U \subset \mathbb{I}$) of a point x , let g be continuous at x , and let $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$ for a suitable finite automaton \mathfrak{A} ; then there exists a mark-up for every base- p expansion of x . Moreover, if $g: [a, b] \rightarrow [0, 1]$ is a continuous function on the closed segment $[a, b]$ then there exist an s -mark-up for right base- p expansion of a and for left base- p expansion of b .*

Corollary 4.8. *In conditions of Proposition 4.6, if the automaton \mathfrak{A} is minimal then $\mathbf{G}(g) \subset \mathbf{LP}(\mathfrak{A})$.*

Proof of Corollary 4.8. Follows immediately from Corollary 2.21 by the definition of mark-up. \square

The following proposition reduces examination of continuous functions computable by a finite automaton \mathfrak{A} for the case when the function is defined on a segment for which there exists a state s of the automaton such that the set of all points from the segment that has s -mark-ups, is dense in the segment; and so values at these points completely specify the function on the segment.

Proposition 4.9. *Let $g: [a, b] \rightarrow [0, 1]$, $[a, b] \subset [0, 1]$, be a continuous function; let $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$ for a suitable automaton \mathfrak{A} whose set of states \mathcal{S} is finite. Then $[a, b]$ is a union of a countably many sub-segments $[a'_j, b'_j] \subset [a, b]$, $a'_j < b'_j$, $j = 1, 2, \dots$ having the following property: For every $j = 1, 2, \dots$ there exists a state $s_q \in \mathcal{S}$, $q = q(j)$, such that the set $M_q([a'_j, b'_j])$ of all points from $[a'_j, b'_j]$ that have s_q -mark-ups is dense in $[a'_j, b'_j]$.*

Proof of Proposition 4.9. For $s \in \mathcal{S}$ denote via $\mathcal{W}^\infty(s)$ the set of all right-infinite words $w \in \mathcal{W}^\infty$ such that $0.w \in (a, b)$ and an s -mark-up for w exists; put $0.\mathcal{W}^\infty(s) = \{0.w : w \in \mathcal{W}^\infty(s)\}$.

Given $s \in \mathcal{S}$ such that $\mathcal{W}^\infty(s) \neq \emptyset$, let $\mathbf{W}(s)$ be intersection of the closure $\overline{\mathbf{W}(s)}$ of $0.\mathcal{W}^\infty(s)$ with (a, b) ; so $\mathbf{W}(s)$ is closed in (a, b) w.r.t. the induced topology on (a, b) and there are only finitely many pairwise distinct $\mathbf{W}(s)$; say, these are $\mathbf{W}(s_1), \dots, \mathbf{W}(s_k)$. Proposition 4.6 implies that $\mathbf{W}(s_1) \cup \dots \cup \mathbf{W}(s_k) = (a, b)$. We argue that for some $\mathbf{W}(s_1), \dots, \mathbf{W}(s_k)$ their interiors $\mathbf{W}(s_1)^\circ, \dots, \mathbf{W}(s_k)^\circ$ are not empty. Indeed, $\mathbf{W}(s_i)^\circ = \overline{\mathbf{W}(s_i)}^\circ \cap (a, b)$ for all $i = 1, 2, \dots, k$; but from Proposition 4.6 it follows that $\overline{\mathbf{W}(s_1)} \cup \dots \cup \overline{\mathbf{W}(s_k)} = [a, b]$ and therefore $\overline{\mathbf{W}(s_1)}^\circ \cup \dots \cup \overline{\mathbf{W}(s_k)}^\circ$ is dense in $[a, b]$ as $[a, b]$ is Baire, cf. e.g. [1, Theorems 6.16–6.17].

As some (without loss of generality we may assume that all) of the interiors $\overline{\mathbf{W}(s_1)}^\circ, \dots, \overline{\mathbf{W}(s_k)}^\circ$ are non-empty, the interiors are countable unions of open intervals: $\overline{\mathbf{W}(s_i)}^\circ = \bigcup_{\ell=1}^\infty (a'_{i\ell}, b'_{i\ell})$, $a'_{i\ell} < b'_{i\ell}$, $(i = 1, 2, \dots, k)$. Therefore $\overline{\mathbf{W}(s_i)} = \bigcup_{\ell=1}^\infty [a'_{i\ell}, b'_{i\ell}]$. This completes the proof as $\mathbf{W}(s_1) \cup \dots \cup \mathbf{W}(s_k) = [a, b]$. \square

Corollary 4.10. *In conditions of Proposition 4.9, the segment $[a, b]$ admits a countable covering by closed sub-segments $[a'_j, b'_j] \subset [a, b]$ such that the graph $\mathbf{G}(g_j)$ of the restriction of the function g to the sub-segment $[a'_j, b'_j]$ lies in $\mathbf{P}(\mathfrak{A}(s)) \subset \mathbf{P}(\mathfrak{A})$ for a suitable sub-automaton $\mathfrak{A}(s)$ of the automaton \mathfrak{A} , $s = s(j) \in \mathcal{S}$.*

Proof of Corollary 4.10. Indeed, the closure of the point set $\{(x; g(x)) : x \in M_q([a'_j, b'_j])\}$ in \mathbb{R}^2 is a graph of the restriction g_j of the function g to the segment $[a'_j, b'_j]$ as g_j is continuous on $[a'_j, b'_j]$. On the other hand the closure must lie in $\mathbf{P}(\mathfrak{A}(s))$ for $s = s_q$ as $g(x) = \lim_{k \rightarrow \infty} \rho(\mathfrak{a}_s(\gamma_0 \dots \gamma_{i_k}))$ where $x = 0.\gamma_0\gamma_1\dots$ and i_0, i_1, \dots is an s -mark-up. Note also that $\mathbf{P}(\mathfrak{A}(s)) \subset \mathbf{P}(\mathfrak{A})$ as every state of the automaton \mathfrak{A} is reachable from its initial state s_0 (since we consider reachable automata only, cf. Subsection 2.3). \square

Note 4.11. From the respective proofs it follows that both Proposition 4.9 and Corollary 4.10 remain true for a continuous function $g: [a, b] \rightarrow \mathbb{S}$ as well as for the case when $[a, b] \subset \mathbb{S}$.

The following theorem shows that we may restrict our considerations of finitely computable continuous functions to the case when computing automata are minimal.

Theorem 4.12. *Given a continuous function $g: [a, b] \rightarrow [0, 1]$, $[a, b] \subset [0, 1]$ such that $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$ for a finite automaton \mathfrak{A} , there exists a countable covering $\{[a'_j, b'_j] \subset [a, b] : j = 1, 2, \dots; a'_j < b'_j\}$ of the segment $[a, b]$ such that for every j the graph $\mathbf{G}(g_j)$ of the restriction g_j of the function g to the segment $[a'_j, b'_j]$ lies in $\mathbf{LP}(\mathfrak{A}_n)$ for a suitable minimal sub-automaton \mathfrak{A}_n of \mathfrak{A} , $n = n(j)$.*

Proof of Theorem 4.12. The state s_q from Proposition 4.9 is either ergodic or transient, see Subsection 2.3. We consider these two cases separately.

Case 1: The state s_q is ergodic. As the set $M_q([a'_j, b'_j])$ from Proposition 4.9 is dense in $[a'_j, b'_j]$ and g_j is continuous, every point $g_j(x)$ for $x \in [a'_j, b'_j]$ is a limit of a sequence $(g(x_i))_{i=0}^\infty$ where $(x_i)_{i=0}^\infty$ is a sequence of points from $M_q([a'_j, b'_j])$ and $(x_i)_{i=0}^\infty$ tends to x as i tends to infinity:

$$x = \lim_{i \rightarrow \infty} x_i; \quad (4.69)$$

$$g_j(x) = \lim_{i \rightarrow \infty} g_j(x_i). \quad (4.70)$$

But $x_i = 0.w_i$ where w_i is a right-infinite word for which there exists an s_q -mark-up (cf. the construction of the set $M_q([a'_j, b'_j])$); therefore from (4.69)–(4.70) it follows now that there exists a sequence $(h_\ell)_{\ell=0}^\infty$ of finite words h_ℓ of strictly increasing lengths such that

$$x = \lim_{\ell \rightarrow \infty} 0.h_\ell; \quad (4.71)$$

$$g_j(x) = \lim_{\ell \rightarrow \infty} \rho(\mathfrak{a}_{s_q}(h_\ell)). \quad (4.72)$$

Indeed, the words h_ℓ are (left) prefixes of words $w_q = \omega_0^{(q)}\omega_1^{(q)}\dots$ that correspond to s_q -mark-up; that is, h_ℓ are of the form $\omega_0^{(q_\ell)}\omega_1^{(q_\ell)}\dots\omega_{r_{q_\ell, k_\ell}}^{(q_\ell)}$ where the sequence $(r_{q_\ell, k_\ell})_{k=0}^\infty$ is the s_q -mark-up of the word w_{q_ℓ} . Now, as the state s_q is ergodic (that is, s_q a state of a certain minimal sub-automaton, say $\mathfrak{A}_q = \mathfrak{A}(s_q)$, of the automaton \mathfrak{A} , cf. Subsection 2.3), then we just mimic the proof of Theorem 2.20 starting with (2.21)–(2.22) and show that $(x, g_j(x)) \in \mathbf{LP}(\mathfrak{A}_q)$.

Case 2: Now let the state s_q from Proposition 4.9 be not ergodic (whence transient). Thus there exists a finite word $u = \alpha_0 \dots \alpha_{k-1}$ such that after the automaton $\tilde{\mathfrak{A}} = \mathfrak{A}(s_q)$ has been feeded by the word u (rightmost letters are feeded to the automaton prior to leftmost ones), the automaton reaches some ergodic state (say t) which is a state of a minimal sub-automaton $\mathfrak{A}' = \mathfrak{A}(t)$, see Subsection 2.3. Note that then all words of the form vu have the same property, for all $v \in \mathcal{W}_\phi$: After being feeded by vu , the automaton reaches some state from the set of states of \mathfrak{A}' due to the minimality of \mathfrak{A}' . Therefore, the set $B_q \subset \mathbb{Z}_p$ of all p -adic integers

whose base- p expansions (cf. Subsection 2.2) are left-infinite words $w \in \mathcal{W}^\infty$ such that if the automaton $\mathfrak{A}(s_q)$ while being fed by the word w reaches at a finite step some ergodic state (that is, reaches a state which is a state of some minimal automaton of \mathfrak{A}) is a union of balls of non-zero radii in \mathbb{Z}_p ; thus, the set B_q is an open subset in \mathbb{Z}_p since every ball of a non-zero radius is open in \mathbb{Z}_p w.r.t. the p -adic topology, cf. Subsection 2.2. Hence the set $A_q = \mathbb{Z}_p \setminus B_q$ is a closed subset of \mathbb{Z}_p ; and the set A_q consists of all p -adic integers such that if the automaton $\mathfrak{A}(s_q)$ is being fed by a left-infinite word that is a base- p expansion of some p -adic integer from A_q , the automaton \mathfrak{A} never reaches an ergodic state. Let P_q be the set of all finite prefixes of words from A_q ; denote \mathbf{P}_q a closure of the set $0.P_q = \{0.w : w \in P_q\}$ in \mathbb{R} .

Claim: *The interior of \mathbf{P}_q is empty* (therefore \mathbf{P}_q is nowhere dense in $[0, 1]$).

Indeed, if not then \mathbf{P}_q contains an open interval (a_q, b_q) . Take a finite non-empty word u such that $a_q < 0.u < b_q$. As $\mathbf{P}_q \supset (a_q, b_q)$ then, given an arbitrary finite non-empty word $v = \alpha_1 \dots \alpha_k$ where $\alpha_k \neq 0$, there exists a sequence $\mathcal{W}(v) = (w_i)_{i=1}^\infty$ of finite non-empty words $w_i \in P_q$ such that $\lim_{i \rightarrow \infty} 0.w_i = 0.uv \in (a_q, b_q)$ (recall that uv is a concatenation of words u and v). Therefore either $uv \in P_q$ (thus $v \in P_q$ by the construction of P_q) or $\mathcal{W}(v)$ contains an infinite subsequence of words of the form $w'_i = u\alpha_1 \dots \alpha'_k(p-1)^{r_i}$ where $\alpha'_k = \alpha_k - 1$, $r_1 < r_2 < \dots$ (recall that $(p-1)^{r_i}$ is a word of length r_i all whose letters are $p-1$); hence by the construction of P_q there exists an infinite sequence $w''_i = \alpha_1 \dots \alpha'_k(p-1)^{r_i}$ over P_q . Thus we conclude that once $n \in \mathbb{N}$, the closure of A_q in \mathbb{Z}_p (thus, the very set A_q itself as it is closed) must either contain n or $-n$ (recall that negative rational integers in \mathbb{Z}_p are exactly that ones whose canonical p -adic expansions have only a finitely many terms with coefficients other than $p-1$, cf. Subsection 2.2). But this implies that $A_q = \mathbb{Z}_p$ as the set $\{\pm n : n \in \mathbb{N}\}$ (where $+$ or $-$ are taken in arbitrary order) is dense in \mathbb{Z}_p . On the other hand, by the construction the set A_q consists of all p -adic integers such that if the automaton $\mathfrak{A}(s_q)$ is being fed by a left-infinite word that is a base- p expansion of some p -adic integer from A_q , the automaton \mathfrak{A} never reaches an ergodic state; therefore the equality $A_q = \mathbb{Z}_p$ contradicts our assumption that s_q is transient (since then there must exist a left-infinite word w such that at a finite step the automaton $\tilde{\mathfrak{A}} = \mathfrak{A}(s_q)$ reaches an ergodic state if being fed by w). This proves our claim.

Denote now via \tilde{f} an automaton function of the automaton $\tilde{\mathfrak{A}} = \mathfrak{A}(s_q)$; and for $k = 1, 2, \dots$ put

$$E'_k(\tilde{f}) = \left\{ \left(\frac{z \bmod p^k}{p^k}; \frac{\tilde{f}(z) \bmod p^k}{p^k} \right) \in \mathbb{I}^2 : z \in \mathbb{Z}_p \setminus A_q = B_q \right\} \quad (4.73)$$

a point set in the unit real square $\mathbb{I}^2 = [0, 1] \times [0, 1]$; then take a union $E'(\tilde{f}) = \cup_{k=1}^\infty E'_k(\tilde{f})$; denote via $\mathbf{P}'(\tilde{\mathfrak{A}}) = \mathbf{P}'(\tilde{f})$ a closure (in topology of \mathbb{R}^2) of the set $E'(\tilde{f})$ (cf. (2.17)). Denote via g_j a restriction of the function g to $[a'_j, b'_j]$. As the function g_j is continuous on $[a'_j, b'_j]$ (cf. Corollary 4.10) and $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$, then necessarily $\mathbf{G}(g_j) \subset \mathbf{P}'(\tilde{\mathfrak{A}})$ since the set \mathbf{P}_q is nowhere dense in $[a'_j, b'_j]$ by Claim 1.

As the set \mathcal{S} of all states of the automaton \mathfrak{A} is finite, there are only finitely many ergodic components in \mathcal{S} ; say they are $\mathcal{S}_1, \dots, \mathcal{S}_m \subset \mathcal{S}$. Given an ergodic component \mathcal{S}_n ($n = 1, 2, \dots, m$) denote

$$E_n = \left\{ \left(\frac{z \bmod p^k}{p^k}; \frac{\tilde{f}(z) \bmod p^k}{p^k} \right) \in \mathbb{I}^2 : z \in B_q, k > k_n(z) \right\}$$

where $k_n(z)$ is the smallest $k \in \mathbb{N}$ such that after the automaton $\tilde{\mathfrak{A}} = \mathfrak{A}(s_q)$ has been fed by the word $\text{wrd}(z \bmod p^{k_n(z)})$, the automaton reaches a state from

\mathcal{S}_n . Then the union $E = \cup_{n=1}^m E_n$ is disjoint and $\mathbf{P}'(\tilde{\mathfrak{A}})$ is a closure of E by (4.73). Therefore $\mathbf{P}'(\tilde{\mathfrak{A}}) = \cup_{n=1}^m \mathbf{E}_n$ where \mathbf{E}_n is a closure of E_n in \mathbb{I}^2 ; hence $\mathbf{G}(g_j) = \cup_{n=1}^m (\mathbf{G}(g_j) \cap \mathbf{E}_n)$. Note that from the definition of $\mathbf{P}(\mathfrak{A})$ (cf. Subsection 2.5) it follows that $\mathbf{E}_n = \mathbf{P}(\mathfrak{A}_n)$ where \mathfrak{A}_n is a minimal sub-automaton (of the automaton \mathfrak{A}) whose set of states is \mathcal{S}_n .

Further, as the function g_j is continuous on $[a'_j, b'_j]$, the set $\mathbf{G}(g_j)$ is closed in \mathbb{I}^2 ; therefore the set $\mathbf{G}_n = \mathbf{G}(g_j) \cap \mathbf{E}_n$ is closed in \mathbb{R}^2 . Hence, the set $\mathbf{R}_n = \{x \in [a'_j, b'_j] : (x, g(x)) \in \mathbf{E}_n\}$ is closed in \mathbb{R} and $[a'_j, b'_j] = \cup_{n=1}^m \mathbf{R}_n$. Now by argument similar to that from the proof of Proposition 4.9 we conclude that some of the interiors \mathbf{R}_n° must be non-empty and hence either of the non-empty interiors is a union of a countably many open intervals. By taking closures of the intervals we see that $[a'_j, b'_j]$ is a union of the closures, that is, $[a'_j, b'_j]$ is a union of a countably many its closed sub-segments $[a'_{j,i}, b'_{j,i}]$ ($i \in \mathbb{N}_0$) of non-zero lengths, and the graph of the restriction $g_{j,i}$ of g_j to either of the sub-segments lies in $\mathbf{E}_n = \mathbf{P}(\mathfrak{A}_n)$ for a suitable $n \in \{1, 2, \dots, m\}$. Now we apply Proposition 4.9 substituting $g_{j,i}$ for g and $[a'_{j,i}, b'_{j,i}]$ for $[a, b]$; but as every s_q from the statement of Proposition 4.9 is now a state of the minimal sub-automaton \mathfrak{A}_n , we now are in conditions of Case 1. Therefore $\mathbf{G}(g_{j,i}) \subset \mathbf{LP}(\mathfrak{A}_n(s_q))$; but $\mathbf{LP}(\mathfrak{A}_n(s)) = \mathbf{LP}(\mathfrak{A}_n(t))$ for all states s, t of the automaton $\mathbf{LP}(\mathfrak{A}_n(s_q))$ due to the minimality of the automaton, cf. Note 2.22.

This finally proves the theorem. \square

Note 4.13. From the proof of Theorem 4.12 it follows that the theorem remains true for a continuous function $g: [a, b] \rightarrow \mathbb{S}$ as well as for the case when $[a, b] \subset \mathbb{S}$.

The following proposition shows that we may if necessary consider only finitely computable continuous functions defined everywhere on the unit segment $[0, 1]$ rather than on sub-segments of $[0, 1]$.

Proposition 4.14 (The similarity). *If a continuous function $g: [a, b] \rightarrow \mathbb{S}$, $[a, b] \subset [0, 1]$, is such that $\mathbf{G}_{[a,b]}(g) \subset \mathbf{P}(\mathfrak{A})$ for a suitable finite automaton $\mathfrak{A} = \mathfrak{A}(s_0)$ then for every $n, m \in \mathbb{N}_0$ such that $m \geq \lfloor \log_p n \rfloor + 1$ and $n/p^m, (n+1)/p^m \in [a, b]$ the function $g_d(x) = (p^m g(d + p^{-m}x)) \bmod 1$, where $d = np^{-m}$, is continuous on $[0, 1]$, and $\mathbf{G}_{[0,1]}(g_d) \subset \mathbf{P}(\mathfrak{A})$.*

Proof of Proposition 4.14. As a base- p expansion of d is $d = 0.\chi_0 \dots \chi_{m-1}00\dots$ then, given a base- p expansion for $x = 0.\zeta_0\zeta_1\dots \in [0, 1]$, a base- p expansion for $d + xp^{-m}$ is $d + xp^{-m} = 0.\chi_0 \dots \chi_{m-1}\zeta_0\zeta_1\dots$ and $d + xp^{-m} \in [a, b]$ for all right-infinite words $\zeta_0\zeta_1\dots$ (thus, for all $x \in [0, 1]$). Therefore if $i_0 < i_1 < i_2 < \dots$ is a mark-up for $\chi_0 \dots \chi_{m-1}\zeta_0\zeta_1\dots$ (cf. Proposition 4.6) then $(j_m = i_{r+m} - m)_{m=0}^\infty$, where $r = \min\{\ell: i_\ell > m\}$, is an s -mark-up of the infinite word $\zeta_0\zeta_1\dots$ for a suitable state $s \in \mathcal{S}$ of the automaton $\mathfrak{A} = \mathfrak{A}(s_0)$ w.r.t. the function g . Hence,

$$\lim_{k \rightarrow \infty} \rho(\mathbf{a}_s(\zeta_0\zeta_1\dots\zeta_{j_k})) \equiv \left(p^m \cdot \left(g \left(d + \frac{x}{p^m} \right) \right) \right) \pmod{1} \quad (4.74)$$

as $\rho(\mathbf{a}_s(\zeta_0\zeta_1\dots\zeta_{j_k})) = (p^m(\rho(\mathbf{a}_s(\chi_0\dots\chi_{m-1}\zeta_0\zeta_1\dots\zeta_{j_k})))) \bmod 1$. By our assumption on reachability of the automaton \mathfrak{A} (cf. Subsection 2.3), there exists a finite word $u = u(s)$ such that the automaton \mathfrak{A} being fed by u reaches the state s and outputs the corresponding finite word $u' = \mathbf{a}_{s_0}(u)$; therefore the automaton $\mathfrak{A} = \mathfrak{A}(s_0)$ being fed by a concatenated finite word $\zeta_0\zeta_1\dots\zeta_{j_k}u$ outputs the concatenated finite word $\mathbf{a}_s(\zeta_0\zeta_1\dots\zeta_{j_k})u'$. But $\lim_{k \rightarrow \infty} \rho(\mathbf{a}_{s_0}(\zeta_0\zeta_1\dots\zeta_{j_k}u)) = \lim_{k \rightarrow \infty} \rho(\mathbf{a}_s(\zeta_0\zeta_1\dots\zeta_{j_k})u') = \lim_{k \rightarrow \infty} \rho(\mathbf{a}_s(\zeta_0\zeta_1\dots\zeta_{j_k}))$ and simultaneously $x = \lim_{k \rightarrow \infty} \rho(\zeta_0\zeta_1\dots\zeta_{j_k}u) = \lim_{k \rightarrow \infty} \rho(\zeta_0\zeta_1\dots\zeta_{j_k})$ since the words u, u' are finite and fixed; therefore $(x; g_d(x) \bmod 1) \in \mathbf{P}(\mathfrak{A})$ for all $x \in [0, 1]$ in view of (4.74).

The function g_d is conjugated to a continuous function by a continuous map and therefore is also continuous: Once $e, h \in [0, 1]$ are such that $|e - h| < p^{-K(L)}$ to ensure that $|g(d + p^{-m}e) - g(d + p^{-m}h)| < p^{-L}$ for a sufficiently large $L \in \mathbb{N}$ then $|g_d(e) - g_d(h)| < p^{-L+m}$. \square

Corollary 4.15. *If a continuous function $g: [a, b] \rightarrow \mathbb{S}$, $[a, b] \subset [0, 1]$, is such that $\mathbf{G}_{(a,b)}(g) \subset \mathbf{P}(\mathfrak{A})$ for a suitable finite automaton $\mathfrak{A} = \mathfrak{A}(s_0)$ then for every $n, m \in \mathbb{N}_0$ such that $m \geq \lfloor \log_p n \rfloor + 1$ and $d = n/p^m \in [a, b]$*

- *the function $g_{d,M}(x) = (p^M g(d + p^{-M}x)) \bmod 1$ is continuous on $[0, 1]$ for all sufficiently large $M \geq m$, and*
- *$\mathbf{G}_{[0,1]}(g_{d,M}) \subset \mathbf{P}(\mathfrak{A})$.*

Proof of Corollary 4.15. Indeed, in the proof of Proposition 4.14 as a base- p expansion for $d = np^{-m}$ just use $0.\chi_0 \dots \chi_{m-1}(0)^{M-m}$ where $M \geq m$ is large enough so that $0.\chi_0 \dots \chi_{m-1}(0)^{M-m-1}1 \in [a, b]$. Note that nowhere in the proof of the proposition we used that some of $\chi_0, \dots, \chi_{m-1}$ are not zero. \square

Note 4.16. Corollary 4.15 shows that given any point $d' \in [a, b]$ and a rational approximation $d = np^{-m}$ of d' , the graph of the function g on a sufficiently small closed neighbourhood $[a', b']$ of the point $d' \neq b'$ is similar to the graph of the function $g_{d,M}$ on $[0, 1]$ where $d = np^{-m}$ and M is large enough.

Summarizing results of the current subsection we may say that while considering a continuous function $g: [a, b] \rightarrow \mathbb{S}$ (where $[a, b] \subset [0, 1]$ or $[a, b] \subset \mathbb{S}$) whose graph $\mathbf{G}(g)$ lies in $\mathbf{P}(\mathfrak{A})$ for some finite automaton \mathfrak{A} one can if necessary assume that the function is defined and continuous on $[0, 1]$ (or on \mathbb{S} except for maybe a single point), the automaton \mathfrak{A} is minimal, the function g is ultimately computable by \mathfrak{A} and that for some state s of \mathfrak{A} the set of all points from $[0, 1]$ which have base- p expansions admitting s -mark-ups is dense in $[0, 1]$ (respectively, in \mathbb{S}).

4.2. Finite computability of compositions. It is clear that a composition of finitely computable continuous functions should be a finitely computable continuous function. The following proposition states this formally and gives some extra information about the graph of a composite finitely computable function.

Proposition 4.17. *Let $[a, b], [c, d] \subset [0, 1]$ and let $g: [a, b] \rightarrow [0, 1]$, $f: [c, d] \rightarrow [0, 1]$ be two continuous functions such that $g([a, b]) \subset [c, d]$ and there exist finite automata \mathfrak{A} and \mathfrak{B} such that $\mathbf{G}_{[a,b]}(g) \subset \mathbf{P}(\mathfrak{A})$, $\mathbf{G}_{[c,d]}(f) \subset \mathbf{P}(\mathfrak{B})$. Then there exists a covering $\{[a'_j, b'_j] \subset [a, b]: j \in J\}$ such that if h_j is a restriction of the composite function $f(g)$ to the sub-interval $[a'_j, b'_j]$ then $\mathbf{G}_{[a'_j, b'_j]}(h_j) \subset \mathbf{P}(\mathfrak{C}_j)$ for every $j \in J$, where \mathfrak{C}_j is a sequential composition of the automaton $\mathfrak{A}(s_j)$ with the automaton $\mathfrak{B}(t_j)$ and s_j, t_j are suitable (depending on j) states of the automata \mathfrak{A} , \mathfrak{B} accordingly.*

Proof of Proposition 4.17. By Note 4.7, for every right-infinite word $w = \gamma_0\gamma_1 \dots \in \mathcal{W}^\infty$ such that $x = 0.w \in (a, b)$ there exists a mark-up (w.r.t. some state s of the finite automaton \mathfrak{A}) i_0, i_1, i_2, \dots ; i.e., $\lim_{k \rightarrow \infty} \rho(\mathbf{a}(w_k)) = g(x)$, where $w_k = \gamma_0\gamma_1 \dots \gamma_{i_k} \in \mathcal{W}$; and if $x = a$ (respectively, $x = b$) then the mark-up exists at least for right (respectively, left) base- p expansion. By the same reason, for $y = g(x) = 0.v$, where $v = \nu_0\nu_1 \dots \in \mathcal{W}^\infty$, there exists a mark-up j_0, j_1, \dots (w.r.t. some state t of the finite automaton \mathfrak{B}) such that $\lim_{n \rightarrow \infty} \rho(\mathbf{b}(v_n)) = g(y)$, where $v_n = \nu_0\nu_1 \dots \nu_{i_n} \in \mathcal{W}$. Now for $m \in \mathbb{N}_0$ denote $N(m) = \min\{k: i_k \geq j_m\}$, consider the sequence $(N(m))_{m=0}^\infty$ and let $q(0) = N(m_0), q(1) = N(m_1), \dots$ be a strictly increasing subsequence of $(N(m))_{m=0}^\infty$. Denote $s(\ell)$ the state the automaton \mathfrak{A} reaches after being feeded by the word $\gamma_{j_{m_\ell}+1}\gamma_{j_{m_\ell}+2} \dots \gamma_{i_{q(\ell)}}$; put

$s(\ell) = s$ if the latter word is empty. As the automaton \mathfrak{A} is finite, there is a state, say s' , that occurs in the sequence $(s(\ell))$ infinitely often. Then the sequence $(j_{m(\ell)}: s(\ell) = s')$ is a mark-up of the word w w.r.t. the automaton $\mathfrak{A}(s')$, and simultaneously the same sequence is a mark-up of the word v w.r.t. the automaton $\mathfrak{B}(t)$. Therefore $\lim_{\ell \rightarrow \infty} \rho(\mathfrak{C}'(\gamma_0 \gamma_1 \dots \gamma_{j_{m(\ell)}})) = f(y) = f(g(x))$, where \mathfrak{C}' is a sequential composition of automata $\mathfrak{A}(s')$ and $\mathfrak{B}(t)$.

By Corollary 4.10, the segment $g([a, b])$ can be covered by a countably many segments $[c_k, d_k]$, $k \in \mathbb{N}$ where for every k there exists a state t_k of the automaton \mathfrak{B} such that the set of all points from $[c_k, d_k]$ whose base- p expansions (w.r.t. the function f) admit t_k -mark-ups is dense in $[c_k, d_k]$. Given a real number $y \in [c_k, d_k]$ and its base- p expansion, in view of Proposition 4.6 there exists a t_k -mark-up of the base- p -expansion. Having this mark-up and by acting as above, we, given $x \in g^{-1}(y)$ find corresponding state s'_k of the automaton \mathfrak{A} and construct a strictly increasing sequence over \mathbb{N} such that the sequence is simultaneously a mark-up for y (w.r.t. t_k and the function f) and for x (w.r.t. s'_k and the function g).

Let s'_1, \dots, s'_r be all pairwise distinct states of the automaton \mathfrak{A} that satisfy the following condition: For every $w, v \in \mathcal{W}^\infty$ such that $0.v \in [a, b]$, $g(0.w) = 0.v$ there exists an s'_i -mark-up (for suitable $i \in \{1, 2, \dots, r\}$) such that the mark-up is a mark-up both for w (w.r.t. s'_i and g) and for v (w.r.t. t_k and f) simultaneously. For $i \in \{1, 2, \dots, r\}$ denote via $\mathcal{W}^\infty(s'_i)$ the set of all infinite words $w \in \mathcal{W}^\infty$ such that there exists an s -mark-up which is a mark-up both for w and for v simultaneously; then proceeding in the same way as in the proof of Proposition 4.9 we conclude that there exists $s' = s'_i$ and a closed subinterval $[a', b']$ such that $W = \mathcal{W}^\infty(s'_i) \cap [a', b']$ is dense in $[a', b']$. But then $g(W)$ is dense in $g([a', b'])$ and $f(g(W))$ is dense in $[f(g([a', b']))]$ as g is continuous on $[a', b']$ and f is continuous on $g([a', b'])$. Therefore for a finite automaton \mathfrak{C}'_{ik} which is a sequential composition of the automata $\mathfrak{A}(s'_i)$ and $\mathfrak{B}(t_k)$ we have that the graph of the restriction h of the function $f(g)$ to $[a', b']$ lies in $\mathbf{P}(\mathfrak{C}'_{ik})$. □

Note 4.18. By arguing as in the proof of Proposition 4.17 the following can be shown: Let $[a, b] \subset [0, 1]$, let $g: [a, b] \rightarrow \mathbb{S}$, $f: [a, b] \rightarrow \mathbb{S}$ be two continuous functions, and let there exist finite automata \mathfrak{A} and \mathfrak{B} such that $\mathbf{G}_{[a, b]}(g) \subset \mathbf{P}(\mathfrak{A})$, $\mathbf{G}_{[a, b]}(f) \subset \mathbf{P}(\mathfrak{B})$. Then there exists a covering $\{[a'_j, b'_j] \subset [a, b]: j \in J\}$ such that if h_j is a restriction of the function $(f + g) \bmod 1$ to the sub-interval $[a'_j, b'_j]$ then $\mathbf{G}_{[a'_j, b'_j]}(h_j) \subset \mathbf{P}(\mathfrak{C}_j)$ for every $j \in J$, where \mathfrak{C}_j is a sum of the automaton $\mathfrak{A}(s_j)$ with the automaton $\mathfrak{B}(t_j)$ and s_j, t_j are suitable (depending on j) states of the automata \mathfrak{A} , \mathfrak{B} accordingly. Here by the sum of automata \mathfrak{A} and \mathfrak{B} we mean a sequential composition of the automata by automaton which has two inputs and a single output and performs addition of p -adic integers. The latter automaton is finite, see Subsection 2.4 and Proposition 2.15. Note also that we may assume that both f and g are defined on an arc of \mathbb{S} rather than on $[a, b]$.

Corollary 4.19. *Given $A, B \in \mathbb{Z}_p \cap \mathbb{Q}$ and continuous finitely computable functions $f, g: [a, b] \rightarrow \mathbb{S}$, there exists a covering $\{[a'_j, b'_j] \subset [a, b]: j \in J\}$ such that the function $Af + Bg$ is finitely computable on every $[a'_j, b'_j]$.*

Comparing Theorem 4.12 with Proposition 4.17 we see that in the class of continuous functions there is no big difference between finite computability and ultimate finite computability since given a finitely computable continuous function on a segment there exists a covering of the segment by sub-segments such that the function is ultimately finitely computable on either of the sub-segments.

5. MAIN THEOREMS

In this section we prove that a graph of any C^2 -smooth finitely computable function $g: [a, b] \rightarrow \mathbb{S}$, $[a, b] \subset [0, 1)$, lies (under a natural association of the half-open interval $[0, 1)$ with the unit circle \mathbb{S}) on a torus winding with a p -adic rational slope; and if \mathfrak{A} is a finite automaton that computes g then necessarily the graph of the automaton contains the whole winding. Moreover, we prove a generalization of this theorem for multivariate functions. To make further proofs (which are somewhat involved) more transparent we begin with a brief (and no too rigorous) outline of their general underlying idea.

Given g as above, fix $x = np^{-m} \in [a, b]$; then for $h \in [0, 1]$ and all sufficiently large ℓ from the differentiability of g it follows that $g(x + p^{-m-\ell}h) = g(x) + g'(x) \cdot p^{-m-\ell}h + p^{-m-t(\ell)}\theta(\ell, h)$, where $|\theta(\ell, h)| \leq 1$ and t is a map from \mathbb{N}_0 to \mathbb{N}_0 such that $p^{t(\ell)} \rightarrow \infty$ faster than $p^\ell \rightarrow \infty$ while $\ell \rightarrow \infty$. Once h is fixed (say, $h = p^{-1}$) then the above equality for large ℓ implies (in view of Proposition 4.17 and Corollary 4.19) that there exists a finite automaton \mathfrak{B}_x which computes $(g'(x)) \bmod 1 = ((g(x + p^{-m-\ell-1}) - g(x))p^{m+\ell+1} - p^{1+\ell-t(\ell)}\theta(\ell, p^{-1})) \bmod 1$ being feeded by an infinite sequence of zero words whose lengths increase unboundedly, i.e., $g'(x) \in \mathbf{P}(\mathfrak{B}_x)$: This is because, speaking loosely, the error term $p^{1+\ell-t(\ell)}\theta(\ell, h)$ makes no perturbations of the infinite output sequence due to the fast growth of $t(\ell)$. But then necessarily $g'(x) \in \mathbb{Z}_p \cap \mathbb{Q}$ by Proposition 4.3. Further Lemma 5.2 proves this fact rigorously.

We then (see Lemma 5.3 below) play similar trick with the second derivative $g''(x)$: As g is two times differentiable and $g'(x) \in \mathbb{Z}_p \cap \mathbb{Q}$, the function $g_1(u) = g(u) - g'(x) \cdot u + c$ of argument $u \in [a, b]$ is also a C^2 -smooth finitely computable function for every $c \in \mathbb{Q} \cap \mathbb{Z}_p$. As $g'_1(x) = 0$, $g''_1(u) = g''(u)$, we have (for all sufficiently large ℓ) that $g_1(x + p^{-m-\ell}h) = g_1(x) + \frac{g''(x)}{2} \cdot p^{-2m-2\ell}h^2 + p^{-2m-t_1(\ell)}\theta_1(\ell, h)$ where $|\theta_1(\ell, h)| \leq 1$, $t_1(\ell) = 2\ell + w(\ell)$, and w is a map from \mathbb{N}_0 to \mathbb{N}_0 such that $w(\ell) \rightarrow \infty$ as $\ell \rightarrow \infty$. From here in a way similar to that of above we deduce that $\frac{g''(x)}{2} \in \mathbb{Z}_p \cap \mathbb{Q}$. But then, if $g''(x) \neq 0$, the argument means that there exists a finite automaton which performs squaring $h \rightarrow h^2$ of every $h \in [0, 1]$ with arbitrarily high accuracy. However as it is well known (cf. Subsection 2.3) no finite automaton can do such squaring; so necessarily $g''(x) = 0$ for all $x = np^{-m} \in [a, b]$. But the set of these x is dense in $[a, b]$; therefore $g''(x) = 0$ for all $x \in [a, b]$ as g'' is continuous on $[a, b]$. Hence g must be affine: $g(u) = g'(x)u + e$ for all $u \in [a, b]$. Note that then necessarily $e \in \mathbb{Z}_p \cap \mathbb{Q}$ since $e = g(0)$ and g is finitely computable, cf. Proposition 4.3. After that by Proposition 4.14 we can ‘stretch’ the graph of the function g from $[a, b]$ to the whole unit circle \mathbb{S} and thus finally obtain a whole cable which lies in the plot of the finite automaton which calculates g . But then by Theorem 3.9 the plot must contain the whole link of torus windings; and the graph $\mathbf{G}_{[a,b]}(g)$ must lie completely on some of these windings. The number of links is finite since every link corresponds to some minimal sub-automaton (see Subsection 2.3 and Theorem 4.12) of the automaton which computes g ; and the number of minimal sub-automata of a finite automaton is clearly a finite. Finally, every such link corresponds to a finite family of complex-valued exponential functions of the form $\psi_k(y) = e^{i(Ay - 2\pi p^k B)}$, $k = 0, 1, 2, \dots$, for suitable $A, B \in \mathbb{Z}_p \cap \mathbb{Q}$ as shown in Corollary 3.13. Figures 12 and 13 illustrate how the graphs of C^2 -functions from the plots of finite automata look like.

Now we proceed with rigorous assertions and proofs.

5.1. The univariate case. Here we show that C^2 -smooth finitely computable functions defined on $[a, b] \subset [0, 1)$ and valued in $[0, 1)$ are only affine ones. Once we associate the half-open interval $[0, 1)$ with a unit circle \mathbb{S} under a natural bijection

we may consider graphs of the functions as subsets on a surface of the unit torus $\mathbb{T}^2 = \mathbb{S} \times \mathbb{S}$. We show that then the graphs lie only on cables of the torus \mathbb{T}^2 , and the slopes of the cables must be p -adic rational integers (i.e., must lie in $\mathbb{Z}_p \cap \mathbb{Q}$), see Subsection 2.6 for definitions of torus knots, cables of torus, and links of knots.

Theorem 5.1. *Consider a finite automaton \mathfrak{A} and a continuous function g with domain $[a, b] \subset [0, 1)$, valuated in $[0, 1)$. Let $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$, let g be two times differentiable on $[a, b]$, and let the second derivative g'' of g be continuous on $[a, b]$. Then there exist $A, B \in \mathbb{Q} \cap \mathbb{Z}_p$ such that $g(x) = (Ax + B) \bmod 1$ for all $x \in [a, b]$; moreover, the graph $\mathbf{G}_{[a, b]}(g)$ of the function g lies completely in the cable $\mathbf{C}(A, B) \subset \mathbf{LP}(\mathfrak{A})$ and $\mathbf{C}(A, \bar{B}) \subset \mathbf{LP}(\mathfrak{A})$ for all $\bar{B} \in \mathbf{C}(B \bmod 1)$.*

Given a finite automaton \mathfrak{A} , there are no more than a finite number of pairwise distinct cables $\mathbf{C}(A, B)$ of the unit torus \mathbb{T}^2 such that $\mathbf{C}(A, B) \subset \mathbf{P}(\mathfrak{A})$ (note that $A, B \in \mathbb{Z}_p \cap \mathbb{Q}$ then).

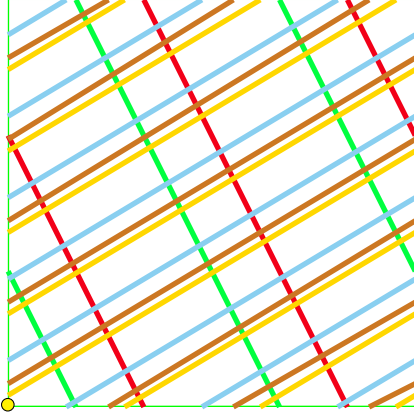


FIGURE 12. The limit plot in \mathbb{R}^2 of an automaton that has two affine subautomata \mathfrak{A} and \mathfrak{B} ; $f_{\mathfrak{A}}(z) = -2z + \frac{1}{3}$ and $f_{\mathfrak{B}}(z) = \frac{3}{5}z + \frac{2}{7}$, where $z \in \mathbb{Z}_2$.

FIGURE 13. The limit plot of the same automaton on the torus \mathbb{T}^2 in \mathbb{R}^3 . The plot consists of two torus links; the links consist of 2 and of 3 knots accordingly.

Lemma 5.2. *Consider a finite automaton \mathfrak{A} and a continuous function g with domain $[a, b] \subset [0, 1)$ valuated in $[0, 1)$. Let $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$ and let g be differentiable at the point $x = np^{-m} \in [a, b)$ where $n \in \mathbb{N}_0$. Then $g'(x) \in \mathbb{Z}_p \cap \mathbb{Q}$.*

Lemma 5.3. *Under conditions of Theorem 5.1 let x be the same as in the statement of Lemma 5.2; then $g''(x) = 0$.*

Proof of Lemma 5.2. Under conditions of the lemma, the right base- p expansion of x is $x = 0.\gamma_0 \dots \gamma_{m-1}00\dots$, for suitable $\gamma_0, \dots, \gamma_{m-1} \in \{0, 1, \dots, p-1\}$. We claim that $(p^m g(x)) \bmod 1 \in \mathbb{Z}_p \cap \mathbb{Q}$. Indeed, as g is continuous and as $x = 0.v0^\infty$ where $v = \gamma_0 \dots \gamma_{m-1}$, there exists an s -mark-up of the right-infinite word $v0^\infty$ w.r.t. some state $s \in \mathcal{S}$ (cf. Note 4.7). That is, there exists a strictly increasing sequence $k_0 < k_1 < \dots$ over \mathbb{N} such that for the infinite sequence of words $w_i = v0^{k_i-m}$ of

strictly increasing lengths k_i (where $i \geq K$ and K is large enough so that $k_i - m > 0$) the following is true:

$$\begin{aligned} \lim_{i \rightarrow \infty} 0.w_i &= x; \\ \lim_{i \rightarrow \infty} 0.\mathbf{a}_s(w_i) &= g(x). \end{aligned}$$

Therefore, the mark-up $(\bar{k}_j = k_{K+j} - m)_{j=0}^\infty$ of the zero right-infinite word 0^∞ is such that (in the notation of Proposition 4.14) the following equalities hold simultaneously

$$\begin{aligned} \lim_{j \rightarrow \infty} 0.0^{\bar{k}_j} &= 0; \\ \lim_{j \rightarrow \infty} 0.\mathbf{a}_s(0^{\bar{k}_j}) &= g_d(0). \end{aligned}$$

Now by combining Proposition 4.14 (or Corollary 4.15 if necessary) and Proposition 4.3 we conclude that $g_d(0) \in \mathbb{Z}_p \cap \mathbb{Q}$ where $d = x = 0.\gamma_0 \dots \gamma_{m-1}$; therefore $(p^m g(x)) \bmod 1 \in \mathbb{Z}_p \cap \mathbb{Q}$ as $g_d(0) = (p^m g(d)) \bmod 1$. Note that if $(n+1)p^{-m} \notin [a, b]$ then we apply Corollary 4.15 rather than Proposition 4.14 and use $g_{d,M}$ instead of g_d and M instead of m here and after.

Take $\ell \in \mathbb{N}$; then by differentiability of g , for all $0 \leq h < 1$ and all sufficiently large $\ell \in \mathbb{N}_0$ we can represent $g(x + p^{-m-\ell}h)$ as

$$g(x + p^{-m-\ell}h) = g(x) + c(x) \cdot p^{-m-\ell}h + p^{-m-t(\ell)}\theta(\ell, h), \quad (5.75)$$

where $c(x) = g'(x)$, $|\theta(\ell, h)| \leq 1$ and t is a map from \mathbb{N}_0 to \mathbb{N}_0 such that $p^{t(\ell)} \rightarrow \infty$ faster than $p^\ell \rightarrow \infty$ while $\ell \rightarrow \infty$. That is, for all sufficiently large ℓ we may represent $t(\ell)$ as $t(\ell) = \ell + w(\ell)$, where w is a map from \mathbb{N}_0 to \mathbb{N}_0 such that $w(\ell) \rightarrow \infty$ as $\ell \rightarrow \infty$.

Further, by Proposition 4.14, the function $\tilde{g}(y) = (p^m g(x + p^{-m}y)) \bmod 1$ is continuous on $[0, 1]$ and $\mathbf{G}_{[0,1]}(\tilde{g}) \subset \mathbf{P}(\mathfrak{A})$. From here by combining Proposition 4.17 and Theorem 3.9 we conclude that there exists a finite automaton \mathfrak{C} such that the graph $\mathbf{G}_{[0,1]}(\tilde{g})$ of the function

$\tilde{g}(y) = (p^m g(x + p^{-m}y) - p^m g(x)) \bmod 1 = ((p^m g(x + p^{-m}y)) \bmod 1 - (p^m g(x)) \bmod 1) \bmod 1$ lies completely in $\mathbf{P}(\mathfrak{C})$.

Indeed, as $(p^m g(x)) \bmod 1 \in \mathbb{Z}_p \cap \mathbb{Q}$ then by (3.49) the graph of the continuous function $y \mapsto y - (p^m g(x)) \bmod 1$ on $[0, 1]$ lies completely in $\mathbf{LP}(\mathfrak{B}) \subset \mathbf{P}(\mathfrak{B})$ for a finite automaton \mathfrak{B} whose automaton function is $f_{\mathfrak{B}}(z) = z - (p^m g(x)) \bmod 1$, ($z \in \mathbb{Z}_p$), and therefore the composite function $\tilde{g}(y)$ is finitely computable on $[0, 1]$, cf. Proposition 4.17. We proceed with this in mind.

We see from (5.75) that for all sufficiently large ℓ and all h the following is true:

$$\tilde{g}(p^{-\ell}h) = (p^m g(x + p^{-m-\ell}h) - p^m g(x)) \bmod 1 = c(x) \cdot p^{-\ell}h + p^{-t(\ell)}\theta(\ell, h). \quad (5.76)$$

Now for the rest of the proof we take (and fix) $h = p^{-1} = 0.1$. Let $0.\alpha_s \alpha_{s+1} \dots$ be a base- p expansion of $(c(x)) \bmod 1$; so $c(x) = \alpha_0 \dots \alpha_{s-1}.\alpha_s \alpha_{s+1} \dots$ is a base- p expansion of $c(x)$. We may assume that $c(x) \geq 0$ since if otherwise we consider the function $(-g) \bmod 1$ which satisfies conditions of the lemma as g satisfies these conditions. If there exists two different base- p expansions for $(c(x)) \bmod 1$ we will consider only one of these. Recall that these expansions are of the form $0.\zeta_1 \dots \zeta_n 0^\infty$ and $0.\zeta_1 \dots \zeta_{n-1} \zeta'_n (p-1)^\infty$ where $\zeta_1, \dots, \zeta_n \in \{0, 1, \dots, p-1\}$, $\zeta_n \neq 0$ and $\zeta'_n = \zeta_n - 1$. Now, if the function $\theta(\ell, p^{-1})$ is non-negative for an infinite number of $\ell \in \mathbb{N}$, then we take the first of the base- p expansions; and we take the second one in the opposite case.

We claim that in all cases mentioned above there exists a strictly increasing sequence \mathcal{L} of $\ell \in \mathbb{N}$ such that, speaking loosely, the term $p^{-t(\ell)}\theta(\ell, h)$ has no affect

on higher order digits of the base- p expansion of the right-hand part of (5.76). In the case when $(c(x)) \bmod 1$ admits only one base- p expansion this follows from the fact that $p^{-t(\ell)}$ tends to 0 faster than $p^{-\ell}$ as we may take for \mathcal{L} all sufficiently large ℓ . In the case when $(c(x)) \bmod 1$ admits two base- p expansions the claim is also true since we consider a right base- p expansion $(c(x)) \bmod 1 = 0.\zeta_1 \dots \zeta_n 0^\infty$ and assume that the function $\theta(\ell, p^{-1})$ in (5.76) is non-negative for an infinite number of $\ell \in \mathbb{N}$: In that case we take for \mathcal{L} all sufficiently large ℓ such that $\theta(\ell, p^{-1}) \geq 0$. When $(c(x)) \bmod 1$ admits two base- p expansions and the function $\theta(\ell, p^{-1})$ is non-negative only for a finite number of $\ell \in \mathbb{N}$, we consider a left base- p expansion $(c(x)) \bmod 1 = 0.\zeta_1 \dots \zeta_{n-1} \zeta'_n (p-1)^\infty$ where $\zeta_1, \dots, \zeta_n \in \{0, 1, \dots, p-1\}$, $\zeta_n \neq 0$ and $\zeta'_n = \zeta_n - 1$. Then there exists infinitely many $\ell \in \mathbb{N}_0$ such that $\theta(\ell, p^{-1}) \leq 0$, and we take for \mathcal{L} all these sufficiently large ℓ .

In other words, if we take $\ell \in \mathcal{L}$, substitute $y = p^{-\ell-1}$ to $\bar{g}(y)$ and apply (5.76) then we get

$$\bar{g}(0.(0)^\ell 1(0)^\infty) = 0.\underbrace{0 \dots 0}_{\ell-s+1} \alpha_0 \dots \alpha_{t_1(\ell)} \delta_{t_1(\ell)+1} \delta_{t_1(\ell)+2} \dots, \quad (5.77)$$

where $\delta_j \in \{0, 1, \dots, p-1\}$ for $j \geq t_1(\ell)+1$, $t_1(\ell) = -\ell + s + t(\ell) = s + w(\ell)$ (note that δ_j depends on ℓ). Further, by Note 4.7 we conclude now that given a right-infinite word u and $\ell \in \mathbb{N}$ there exists an s -mark-up of the word $0^\ell u$ w.r.t. the function \bar{g} where s is a suitable (depending on u and ℓ) state of a finite automaton \mathfrak{C} which is a sequential composition of the automaton \mathfrak{A} with the automaton \mathfrak{B} . This means in particular that given an infinite word $v(\ell) = 0^\ell 100 \dots$, for any $\ell \in \mathcal{L}$ there exists a mark-up (w.r.t. a suitable state $s = s(v(\ell))$ of the automaton \mathfrak{C} , cf. Proposition 4.6) $i_0(\ell), i_1(\ell), i_2(\ell), \dots$ of the word $v(\ell)$. As a total number of states of the automaton \mathfrak{C} is finite, at least one state, say s' , in the sequence $(s(v(\ell)) : \ell \in \mathcal{L})$ occurs infinitely many times. Denote $\mathfrak{C}' = \mathfrak{C}(s')$ (then \mathfrak{C}' is a finite automaton as well) and consider an infinite strictly increasing sequence $\mathcal{L}' = (\ell' : s(v(\ell')) = s' ; \ell' \in \mathcal{L})$.

Given a term ℓ' of the latter sequence \mathcal{L}' take the smallest $k \in \mathbb{N}_0$ such that $i_k(\ell') > t(\ell')$; denote via $s(\ell')$ the state the automaton \mathfrak{C}' reaches after being fed by the word $0^{i_k(\ell')-t(\ell')}$. As the number of states of the automaton \mathfrak{C}' is finite, in the infinite sequence $(s(\ell'))$ at least one term, say \bar{s} , occurs infinitely many times. Consider an infinite sequence $(\ell'_j)_{j=0}^\infty$ such that $s(\ell'_j) = \bar{s}$ and consider an automaton $\mathfrak{C}'(\bar{s})$ (whence the latter automaton is finite also). If the automaton $\mathfrak{C}'(\bar{s})$ is being fed by the word $0^{\ell'_j} 10^{w(\ell'_j)}$ then the automaton outputs the word $q_j = \sigma_0^{(j)} \dots \sigma_{t(\ell'_j)}^{(j)}$; therefore being fed by the word $0^{w(\ell'_j)}$ the automaton outputs the word $q'_j = \sigma_{\ell'_j-s+1}^{(j)} \dots \sigma_{t(\ell'_j)}^{(j)}$ of length $L_j = w(\ell'_j) - s$. As $w(\ell) \rightarrow \infty$ while $\ell \rightarrow \infty$ we may assume without loss of generality that the sequence (L_j) is strictly increasing (since if otherwise we consider a subsequence $(j_i)_{i=0}^\infty$ of the sequence (j) such that the sequence $(L_{j_i})_{i=0}^\infty$). Now by mimic the proof of Proposition 4.3 we show that the sequence $(0.q'_j)$ has only finitely many limit points and all these limit points are in $\mathbb{Z}_p \cap \mathbb{Q}$. But from (5.77) it follows that $\lim_{j \rightarrow \infty} 0.q'_j = (c(x)) \bmod 1$; therefore $(c(x)) \bmod 1 \in \mathbb{Z}_p \cap \mathbb{Q}$ and thus $c(x) = g'(x) \in \mathbb{Z}_p \cap \mathbb{Q}$. \square

Proof of Lemma 5.3. Let x be as in the statement of Lemma 5.2; i.e., let the right base- p expansion of x be as in the proof of Lemma 5.2. Then $g'(x) \in \mathbb{Q} \cap \mathbb{Z}_p$ by Lemma 5.2.

Consider the function $g_1(u) = g(u) - g'(x) \cdot u + c$ of argument $u \in [a, b]$ where $c \in \mathbb{Q} \cap \mathbb{Z}_p$; then g_1 is two times differentiable on $[a, b]$ and $g'_1(x) = 0$, $g''_1(u) = g''(u)$ for all $u \in [a, b]$. As g_1 is continuous on $[a, b]$, the constant c may be taken so that $g_1(u) \in [0, 1]$ for all u from a sufficiently small closed neighborhood $[a_1, b_1]$ of x .

We are going to prove that $g_1''(x) = 0$ for all $x \in [a, b]$. Note that if $g_1''(x) \neq 0$ for some $x \in [a, b]$ then g_1'' does not change its sign on a sufficiently small neighborhood $(a_2, b_2) \subset [a_1, b_1]$ of x . Indeed, if not, then there exist two infinite sequences, $(\tilde{x}_i)_{i=0}^\infty$ and $(\hat{x}_i)_{i=0}^\infty$ such that all the terms of either sequence are pairwise distinct, $\lim_{i \rightarrow \infty} \tilde{x}_i = \lim_{i \rightarrow \infty} \hat{x}_i = x$, and $g_1''(\tilde{x}_i) \geq 0$, $g_1''(\hat{x}_i) \leq 0$ for all $i \in \mathbb{N}_0$. But as $\lim_{i \rightarrow \infty} g_1''(\tilde{x}_i) = \lim_{i \rightarrow \infty} g_1''(\hat{x}_i) = g_1''(x)$ (since g_1'' is continuous at x) then necessarily $g_1''(x) = 0$; but this contradicts our assumption that $g_1''(x) \neq 0$. We therefore may assume that $g_1''(u) \geq 0$ for all $u \in [a_2, b_2]$; otherwise consider the function $1 - g_1$ rather than g_1 .

Finally by Corollary 4.19 we conclude that g_1 is finitely computable on a sufficiently small closed neighbourhood $U \subset [a, b]$ of x . Further we use g for g_1 and $[a, b]$ for U without risk of misunderstanding. Thus we have:

- (i) g is finitely computable on $[a, b] \ni x$;
- (ii) g is two times differentiable on $[a, b]$;
- (iii) g'' is continuous on $[a, b]$;
- (iv) $g'' \geq 0$ on $[a, b]$;
- (v) $g'(x) = 0$;

Now, since g is two times differentiable on $[a, b]$, for all $0 \leq h \leq 1$ and all sufficiently large $\ell \in \mathbb{N}_0$ we can represent $g(x + p^{-m-\ell-1}h)$ as

$$g(x + p^{-m-\ell}h) = g(x) + C(x) \cdot p^{-2m-2\ell}h^2 + p^{-2m-t(\ell)}\theta(\ell, h), \quad (5.78)$$

where $C(x)$ stands for $\frac{g''(x)}{2}$, $|\theta(\ell, h)| \leq 1$, $t(\ell) = 2\ell + w(\ell)$, and w is a map from \mathbb{N}_0 to \mathbb{N}_0 such that $w(\ell) \rightarrow \infty$ as $\ell \rightarrow \infty$.

Claim 1: $C(x) \in \mathbb{Z}_p \cap \mathbb{Q}$. We prove that by mimic of the respective part of the proof of Lemma 5.2. Firstly we show that $(p^m g(x)) \bmod 1 \in \mathbb{Z}_p \cap \mathbb{Q}$ as in the proof of Lemma 5.2; thus considering a function $\bar{g}(y) = (p^m g(x + p^{-m}y) - p^m g(x)) \bmod 1$ we see that

$$\bar{g}(p^{-\ell}h) = (p^m g(x + p^{-m-\ell}h) - p^m g(x)) \bmod 1 = C(x) \cdot p^{-m-2\ell}h^2 + p^{-m-t(\ell)}\theta(\ell, h) \quad (5.79)$$

for all sufficiently large ℓ .

Let $0.\alpha_s\alpha_{s+1}\dots$ be a base- p expansion of $(C(x)) \bmod 1$ (we may take either of the expansions if there exist two different ones); so $C(x) = \alpha_0\dots\alpha_{s-1}.\alpha_s\alpha_{s+1}\dots$ is a base- p expansion of $C(x)$. Take $h = 1$; then for all sufficiently large ℓ the base- p expansion of the right-hand part of (5.79) is of the form

$$0.\underbrace{0\dots 0}_{m+2\ell-s}\alpha_0\dots\alpha_{t_1(\ell)}\delta_{t_1(\ell)+1}\delta_{t_1(\ell)+2}\dots \quad (5.80)$$

where $\delta_j \in \{0, 1, \dots, p-1\}$ for $j \geq t_1(\ell) + 1 = t(\ell) - m - 2\ell + s = w(\ell) - m + s$ depend on ℓ .

The function $(p^m g(x + p^{-m}z) - p^m g(x)) \bmod 1$ of argument z is continuous and finitely computable on $[0, 1]$ by a finite automaton \mathfrak{C} . Now considering an infinite word $0^\ell 10^\infty$ with the corresponding mark-up we prove in the same way as in Lemma 5.2 that the corresponding sequence of finite output words of the automaton \mathfrak{C} is a sequence of initial finite sub-words of the infinite word $0^{m+2\ell-s}\alpha_0\alpha_1\dots$ and then deduce as in the proof of Lemma 5.2 that $C(x) \in \mathbb{Z}_p \cap \mathbb{Q}$ (note that given $x = np^{-m}$ we may always take m so that $m + 2\ell - s > \ell$ without altering the value of x just by multiplying both numerator and denominator by a suitable power of p).

Claim 2: Now we prove that $C(x) = 0$. Assume that $C(x) \neq 0$; that is, that $g''(x) \neq 0$. Let $p^c = |C(x)|_p$, $c \in \mathbb{Z}$, be a p -adic absolute value of $C(x)$; therefore $C(x) = qp^{-c}$, where $q \in \mathbb{Z}_p$, q is a unity of \mathbb{Z}_p , cf. Subsection 2.2. By Claim 1, $C(x) \in \mathbb{Z}_p \cap \mathbb{Q}$, so necessarily $c \leq 0$ and $q \in \mathbb{Q}$; whence $q \in \mathbb{Z}_p \cap \mathbb{Q}$ and thus $q^{-1} \in \mathbb{Z}_p \cap \mathbb{Q}$ as q is a unity. Therefore the function $\bar{g}(y) = (q^{-1}(p^m g(x + p^{-m}y) +$

$p^m g(x)) \bmod 1) \bmod 1$ of argument $y \in [0, 1]$ is finitely computable on $[0, 1]$ (say, by the automaton \mathfrak{B}): This follows from Propositions 4.14, 4.17, and Corollary 4.19. Now by (5.79) we conclude that

$$(q^{-1}(p^m g(x + p^{-m-\ell}h) + p^m g(x)) \bmod 1) \bmod 1 = p^{-k-2\ell}h^2 + p^{-m-t_1(\ell)}\theta_1(\ell, h), \quad (5.81)$$

where $k = c + m \geq 0$ (we may assume that the inequality is true just by taking m sufficiently large by multiplying both numerator and denominator by a suitable power of p and thus without altering the value of x), $|\theta_1(\ell, h)| \leq 1$, $t_1(\ell) = 2\ell + w_1(\ell)$, and w_1 is a map from \mathbb{N}_0 to \mathbb{N}_0 such that $w_1(\ell) \rightarrow \infty$ as $\ell \rightarrow \infty$.

Further, given $n \in \mathbb{N}$ and a word $v_n = \chi_0 \dots \chi_{n-1} \in \mathcal{W}$ and taking $y = p^{-\ell}h$ with $h = 0.v_n 0^\infty$ we have that $(p^{-\ell}h; \check{g}(p^{-\ell}h)) \in \mathbf{P}(\mathfrak{B})$. Let $i_0(\ell, v_n) < i_1(\ell, v_n) < i_2(\ell, v_n) < \dots$ be corresponding mark-up of the infinite word $0^\ell v_n 0^\infty$ (the latter infinite word corresponds to $y = p^{-\ell}h$ once $h = 0.v_n 0^\infty$). Take r the smallest so that $i_r = i_r(\ell, v_n) > t_1(\ell) + m$; denote $s(\ell, v_n)$ the state the automaton \mathfrak{B} reaches after being fed by the word $0^{i_r(\ell, v_n)-k-2\ell-2n}$. As the number of states of the automaton \mathfrak{B} is finite, in the sequence $(s(\ell, v_n))_{\ell=1}^\infty$ at least one state, say $\bar{s}(v_n)$, occurs infinitely many times. Consider a strictly increasing sequence $\mathcal{L} = (\ell_j \in \mathbb{N} : s(\ell_j, v_n) = \bar{s}(v_n))_{j=0}^\infty$; then once $w_1(\ell_j) > 2n + r$, the automaton $\mathfrak{B}(s(\ell_j, v_n)) = \mathfrak{B}(\bar{s}(v_n))$, being fed by the word $0^{\ell_j} v_n 0^{k+\ell_j+n}$, outputs the word $\zeta_0^{(j)} \dots \zeta_{k+2\ell_j-1}^{(j)} \xi_0^{(j)} \dots \xi_{2n-1}^{(j)}$. From (5.81) it follows that $(\lim_{j \rightarrow \infty} (p^{k+2\ell_j} \cdot 0.\zeta_0^{(j)} \dots \zeta_{k+2\ell_j-1}^{(j)} \xi_0^{(j)} \dots \xi_{2n-1}^{(j)}) \bmod 1 = h^2$. Therefore $(\lim_{j \rightarrow \infty} 0.\xi_0^{(j)} \dots \xi_{2n-1}^{(j)}) \bmod 1 = h^2 = 0.\xi_0 \dots \xi_{2n-1}$ where

$$\xi_0 p^{2n-1} + \xi_1 p^{2n-2} + \dots + \xi_{2n-1} = (\chi_0 p^{n-1} + \chi_1 p^{n-2} + \dots + \chi_{n-1})^2$$

(in other words, $\xi_0 \xi_1 \dots \xi_{2n-1}$ is a base- p expansion of the square of the number whose base- p expansion is $v_n = \chi_0 \dots \chi_{n-1}$). Thus necessarily $\xi_0^{(j)} = \xi_0, \dots, \xi_{2n-1}^{(j)} = \xi_{2n-1}$ for all sufficiently large j . But $(p^{-\ell}h; \check{g}(p^{-\ell}h)) \in \mathbf{P}(\mathfrak{B})$ for all ℓ ; thus by Proposition 2.25, $((p^{k+\ell_j}h) \bmod 1; (p^{k+2\ell_j}\check{g}(p^{-\ell_j}h)) \bmod 1) \in \mathbf{P}(\mathfrak{B})$ for all $j \in \mathbb{N}_0$. Therefore for all sufficiently large j (such that $k + \ell_j > n$) we have that $(0; 0.\xi_0 \dots \xi_{2n-1}) \in \mathbf{P}(\mathfrak{B})$ since $h = 0.v_n 0^\infty$. In other words, as the automaton $\mathfrak{B}(s(\ell_j, v_n)) = \mathfrak{B}(\bar{s}(v_n))$, being fed by the word $0^{\ell_j} v_n 0^{k+\ell_j+n}$, outputs the word $\zeta_0^{(j)} \dots \zeta_{k+2\ell_j-1}^{(j)} \xi_0 \dots \xi_{2n-1}$ once j is sufficiently large, $k + \ell_j > n$, the automaton $\mathfrak{B}(\bar{s}(v_n))$, being fed by the zero word 0^{2n} , outputs the word $\xi_0 \xi_1 \dots \xi_{2n-1}$. This means that, given an arbitrary number $N \in \mathbb{N}_0$ whose base- p expansion (where higher order digits might be 0) is of length n , n being sufficiently large, there exists a state s of the finite automaton \mathfrak{B} such that the automaton $\mathfrak{B}(s)$, being fed by a zero sequence of length $2n$, outputs a word (of length $2n$) that is a base- p expansion of N^2 . But this is not possible since it is well known that squaring is not possible by a finite automaton (cf., e.g., [8, Theorem 2.2.3] or [29, Proposition 7.1.6]); however, a short proof follows.

As the automaton \mathfrak{B} is finite, then there are only finitely many sub-automata $\mathfrak{B}(s(\ell, v_n))$. But any finite automaton, being fed by a sufficiently long zero word 0^L outputs the word of the form $u_1(u_2)^M u_3$, where $M = M(L) \in \mathbb{N}$, $u_2 \in \mathcal{W}$, $u_1, u_3 \in \mathcal{W}_\phi$, and the words u_1, u_2, u_3 are completely determined by the finite automaton, u_1 is a right prefix of u_2 , cf. Lemma 2.10. But given finitely many words $u_{1,i}, u_{2,i}, u_{3,i}$ of that sort, $i = 0, 1, 2, \dots, K$, there exist infinitely many words $\xi_0 \xi_1 \dots \xi_{2n-1}$ which are base- p expansions of squares of numbers from \mathbb{N}_0 and which are not of the form $u_{1,i} u_{2,i}^M u_{3,i}$, $i = 1, 2, \dots, K$, $M = 1, 2, \dots$.

The contradiction proves that $C(x) = 0$; therefore, $g''(x) = 0$.

□

Proof of Theorem 5.1. We already have proved that $g''(x) = 0$ if $x = np^{-m} \in [a, b]$, where $n \in \mathbb{N}_0$, $m \geq \lfloor \log_p n \rfloor + 1$. But the set of all these x is dense in $[a, b]$, so, as the second derivative g'' is continuous on $[a, b]$ by the condition of the theorem under proof, g'' must vanish everywhere on $[a, b]$; therefore, $g' = \text{const}$. But this implies that there exist $A, B \in \mathbb{R}$ such that $g(x) = Ax + B$ for all $x \in [a, b]$ and $g'(x) = A$ for all $x \in [a, b]$. From Lemma 5.2 it follows now that $A \in \mathbb{Z}_p \cap \mathbb{Q}$. Now taking an arbitrary number $y \in (a, b) \cap \mathbb{Z}_p \cap \mathbb{Q}$ we see that $g(y) \in \mathbb{Z}_p \cap \mathbb{Q}$ by Proposition 4.3; hence $g(y) - Ay = B$ must be also in $\mathbb{Z}_p \cap \mathbb{Q}$ as $Ay \in \mathbb{Z}_p \cap \mathbb{Q}$.

Now we will prove that $\mathbf{C}(A, B) \subset \mathbf{LP}(\mathfrak{A})$. To begin with, we note that by Theorem 4.12 there exists a minimal sub-automaton \mathfrak{A}' and a segment $[a', b'] \subset [a, b]$ such that $\mathbf{G}_{[a', b']}(g) \subset \mathbf{LP}(\mathfrak{A}')$. Taking $d \in (a', b')$ as in the statement of Proposition 4.14, we conclude that the graph $\mathbf{G}_{[0, 1]}(g_d)$ of the function $g_d(x) = (Ax + An + p^m B) \bmod 1$ on $[0, 1]$ lies completely in $\mathbf{P}(\mathfrak{A}')$; thus $\mathbf{G}_{[0, 1]}(g_d) = \{(x; g_d(x)) : x \in [0, 1]\} \subset \mathbf{LP}(\mathfrak{A}')$ by Corollary 4.8. $An \in \mathbb{Z}$; that is, $p^m a \leq n < p^m b$. As $A \in \mathbb{Z}_p \cap \mathbb{Q}$ then $A = P/Q$ for suitable $P \in \mathbb{Z}$, $Q \in \mathbb{N}$. Now given arbitrary $R \in \{0, 1, \dots, Q-1\}$ we take n and m so that $d = p^{-m}n$ satisfies conditions of Proposition 4.14 (that is, $p^m a \leq n < p^m b$) and $n = LQ + R \in \{0, 1, \dots, p^m - 1\}$ for a suitable $L \in \mathbb{N}_0$ and conclude that

$$\{(x; g_d(x)) : x \in [0, 1]\} = \{(x; (Ax + AR + p^m B) \bmod 1) : x \in [0, 1]\} \subset \mathbf{LP}(\mathfrak{A}')$$

Given arbitrary $R \in \{0, 1, \dots, Q-1\}$, the above inclusion holds for all sufficiently large m ; therefore due the structure of $\mathbf{C}(B)$ (cf. Subsection 3.1) the following inclusion holds for every $R \in \{0, 1, \dots, Q-1\}$ and every $B' \in \mathbf{C}(B)$:

$$\{(x; (Ax + AR + B') \bmod 1) : x \in [0, 1]\} \subset \mathbf{LP}(\mathfrak{A}').$$

But $\bigcup_{R=0}^{Q-1} \{(x; (Ax + AR + B') \bmod 1) : x \in [0, 1]\} = \{((x \bmod 1; (Ax + B') \bmod 1) : x \in \mathbb{R}) = \mathbf{C}(A, B')$; therefore we have shown that $\mathbf{C}(A, B') \subset \mathbf{LP}(\mathfrak{A}')$ for all $B' \in \mathbf{C}(B \bmod 1)$. That is, $\mathbf{LP}(\mathfrak{A}')$ contains the whole link of cables $\mathbf{C}(A, B')$ for all $B' \in \mathbf{C}(B)$ (i.e., contains $\mathbf{LP}(F)$ where $F: z \mapsto Az + B$, $z \in \mathbb{Z}_p$, cf. Theorem 3.9) and $\mathbf{G}_{[a, b]}(g)$ lies completely in a suitable cable of the link. This proves the first claim of Theorem 5.1 since $\mathbf{LP}(\mathfrak{A}') \subset \mathbf{LP}(\mathfrak{A})$, cf. Note 2.23.

To prove the second claim, given a finite automaton \mathfrak{A} consider all cables $\mathbf{C}(A, B)$ such that $\mathbf{C}(A, B) = \{(y \bmod 1; (Ay + B) \bmod 1) : y \in \mathbb{R}\} \subset \mathbf{P}(\mathfrak{A})$; whence by the first claim of the theorem all these cables lie in $\mathbf{LP}(\mathfrak{A})$. Moreover, as we have shown during the proof of the first claim of the theorem, for either of the cables $\mathbf{C}(A, B)$ there exists a minimal sub-automaton $\mathfrak{A}'_{A, B}$ of the automaton \mathfrak{A} such that $\mathbf{C}(A, B) \subset \mathfrak{A}'_{A, B}$. The cables cross zero meridian $\mathbf{O} = \{(0; t \bmod 1) : t \in \mathbb{R}\} \subset \mathbb{T}^2$ of the torus \mathbb{T}^2 only when $y \bmod 1 = 0$; therefore the point set \mathbf{S} of all the points where the cables cross zero meridian consists of the points of the form $(0; e)$ where $e \in \mathfrak{a}(0)$ and \mathbf{S} contains all the points of the form $(0; B \bmod 1)$ where B are constant terms of the cables. As $\mathfrak{a}(0)$ is a finite set (cf. Proposition 4.3), there are no more than a finite number of pairwise distinct numbers $B \bmod 1$ (note that cables with equal slopes whose constant terms are congruent modulo 1 coincide). Now taking $y \in \mathbb{Z}$ we see that all the points of the form $(0; (Ay + B) \bmod 1)$ of the cables belong to zero meridian and therefore to the finite set $\{(0; r) : r \in \mathfrak{a}(0)\}$; hence, there exist no more than a finite number of pairwise distinct numbers $Ay \bmod 1$ where y ranges over rational integers \mathbb{Z} and A are slopes of the cables from $\mathbf{P}(\mathfrak{A})$. Thus if there exists an infinite number of cables in $\mathbf{P}(\mathfrak{A})$ then there exists a minimal sub-automaton \mathfrak{A}' of the automaton \mathfrak{A} such that $\mathbf{LP}(\mathfrak{A}')$ contains an infinite number of cables of the form $\mathbf{C}(AC, B)$ with A, B fixed and C ranging through an infinite subset \mathbf{C} of \mathbb{Z} so that $AC \bmod 1$ are all equal one to another. Therefore for the rest of the proof we may (and will) assume that the automaton \mathfrak{A} is minimal.

By the first claim of the theorem, $A \in \mathbb{Z}_p \cap \mathbb{Q}$; so there exists a unique representation of A in the form

$$A = c + \frac{d}{p^t - 1}$$

where $t \in \mathbb{N}$ is a period length of A , $c \in \mathbb{Z}$, and $d \in \{0, 1, \dots, p^t - 2\}$, cf. Proposition 2.2 and Note 2.4. Therefore \mathbf{C} must contain an infinite subset of numbers from the coset $q + (p^t - 1) \cdot \mathbb{Z}$ for a suitable $q \in \{0, 1, \dots, p^t - 2\}$ since $AC_1 \equiv AC_2 \pmod{1}$ implies $A(C_1 - C_2) \equiv 0 \pmod{1}$, i.e., $A(C_1 - C_2) \in \mathbb{Z}$. Thus from the assumption that there are infinitely many pairwise distinct cables in $\mathbf{P}(\mathfrak{A})$ it follows that then in $\mathbf{LP}(\mathfrak{A})$ there exist infinitely many cables of the form $\mathbf{C}(D + E, B)$ with B, E fixed ($B \in \mathbb{Z}_p \cap \mathbb{Q}$, $E \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1)$) and D running through an infinite subset $\mathbf{D} \subset \mathbb{Z}$. By considering $-f_{\mathfrak{A}}$ (and the corresponding finite automaton) if necessary we may assume that \mathbf{D} is an infinite subset of \mathbb{N} . Therefore, \mathbf{D} constitutes a strictly increasing sequence $(D_i)_{i=0}^{\infty}$ of natural numbers. Now take arbitrary $u \in [0, 1)$ and consider a sequence $x_i = uD_i^{-1}$. As the sequence (D_i) is strictly increasing, $\lim_{i \rightarrow \infty} x_i = 0$; therefore $\lim_{i \rightarrow \infty} (x_i; (D_i x_i + E x_i + B) \bmod 1) = (0; (u + B) \bmod 1) \in \mathbf{LP}(\mathfrak{A})$ as $(x_i; (u + E x_i + B) \bmod 1) \in \mathbf{C}(D_i + E, B) \subset \mathbf{LP}(\mathfrak{A})$ and $\mathbf{LP}(\mathfrak{A})$ is closed in \mathbb{T}^2 , cf. Corollary 2.21. Thus we have proved that zero meridian $\mathbf{O} = \{(0; y) : y \in [0, 1)\}$ of the torus \mathbb{T}^2 lies completely in $\mathbf{LP}(\mathfrak{A})$.

On the other hand, if $(0; y) \in \mathbf{LP}(\mathfrak{A})$ then $y \in \mathfrak{a}(0)$ by definitions of $\mathbf{LP}(\mathfrak{A})$ and $\mathfrak{a}(0)$, see Subsections 2.5 and 4.1; but there are only finitely many points in $\mathfrak{a}(0)$ by Proposition 4.3. The contradiction proves the second claim of the theorem. \square

5.2. The multivariate case. In this subsection we are going to extend Theorem 5.1 for the case of finite automata with multiply inputs/outputs. Note that actually an automaton over alphabet $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ with m inputs and n outputs can be considered as a letter-to-letter transducer with a single input over the alphabet $\{0, 1, \dots, p^m - 1\}$ and a single output over the alphabet $\{0, 1, \dots, p^n - 1\}$; therefore the plot of that automaton is a closed subset of the unit square \mathbb{I}^2 . We however are going to consider plots of automata of that sort as subsets of multidimensional unit hypercube \mathbb{I}^{m+n} . Therefore automata functions of such automata are 1-Lipschitz mappings from \mathbb{Z}_p^m to \mathbb{Z}_p^n , see Subsection 2.4; and vice versa, every 1-Lipschitz mapping from $F: \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p^n$ is an automaton function of a suitable automaton \mathfrak{A} with m inputs and n outputs over the alphabet \mathbb{F}_p . Note that $F = (F_1; \dots; F_m)$ where $F_k: \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p$ ($k = 1, 2, \dots, m$) is 1-Lipschitz and therefore is an automaton function of an automaton with m inputs and a single output.

Now we re-state our definition of a (limit) plot for that case of automata with m inputs and n outputs.

Definition 5.4 (Automata plots, the multivariate case). Given an automaton function $F = F_{\mathfrak{A}}: \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p^n$ define a set $\mathbf{P}(F_{\mathfrak{A}})$ of points of \mathbb{R}^{m+n} as follows: For $k = 1, 2, \dots$ denote

$$E_k(F) = \left\{ \left(\frac{\mathbf{z} \bmod p^k}{p^k}; \frac{F(\mathbf{z}) \bmod p^k}{p^k} \right) \in \mathbb{I}^{m+n} : \mathbf{z} \in \mathbb{Z}_p^m \right\} \quad (5.82)$$

a point set in a unit real hypercube \mathbb{I}^{m+n} ; here given $\mathbf{y} = (y_1; \dots; y_q) \in \mathbb{Z}_p^q$ we put

$$\frac{\mathbf{y} \bmod p^k}{p^k} = \left(\frac{y_1 \bmod p^k}{p^k}; \dots; \frac{y_q \bmod p^k}{p^k} \right) \in (\mathbb{Z}/p^k\mathbb{Z})^q.$$

Then take a union $E(F) = \bigcup_{k=1}^{\infty} E_k(F)$ and denote via $\mathbf{P}(F) = \mathbf{P}(\mathfrak{A})$ a closure (in topology of \mathbb{R}^{m+n}) of the set $E(F)$.

Given an automaton \mathfrak{A} , we call a *plot of the automaton* \mathfrak{A} the set $\mathbf{P}(\mathfrak{A})$. We call a *limit plot* of the automaton \mathfrak{A} the point set $\mathbf{LP}(\mathfrak{A})$ which is defined as follows:

A point $(\mathbf{x}; \mathbf{y}) \in \mathbb{R}^{m+n}$ lies in $\mathbf{LP}(\mathfrak{A})$ if and only if there exist $\mathbf{z} \in \mathbb{Z}_p^m$ and a strictly increasing infinite sequence $k_1 < k_2 < \dots$ of numbers from \mathbb{N} such that simultaneously

$$\lim_{i \rightarrow \infty} \frac{\mathbf{z} \bmod p^{k_i}}{p^{k_i}} = \mathbf{x}; \quad \lim_{i \rightarrow \infty} \frac{F_{\mathfrak{A}}(\mathbf{z}) \bmod p^{k_i}}{p^{k_i}} = \mathbf{y}. \quad (5.83)$$

To put it in other words, at every step a letter-to-letter transducer \mathfrak{A} (which has m inputs and n outputs over a p -symbol alphabet \mathbb{F}_p)

- obtains a vector $\mathbf{a} = (\alpha^{(1)}; \dots, \alpha^{(m)}) \in \mathbb{F}_p^m$ (each i -th letter $\alpha^{(i)}$ is sent accordingly to the i -th input of the automaton, $i = 1, 2, \dots, m$),
- outputs a vector $\mathbf{b} = (\beta^{(1)}; \dots, \beta^{(n)}) \in \mathbb{F}_p^n$ (each j -th output of the automaton outputs accordingly the letter $\beta^{(j)}$, $i = 1, 2, \dots, n$) which depends both on the current state and on the input vector \mathbf{a} ,
- reaches the next state (which depends both on \mathbf{a} and on the current state).

Then the routine repeats. Therefore after k steps the automaton \mathfrak{A} transforms the input m -tuple $\mathbf{w} = (w_1; \dots; w_m)$ of k -letter words $w_i = \alpha_k^{(i)} \dots \alpha_1^{(i)}$ ($i = 1, 2, \dots, m$) into the output n -tuple $\mathbf{v} = \mathbf{a}(\mathbf{w}) = (v_1; \dots; v_n)$ of k -letter words $v_j = \mathbf{a}^{(j)}(\mathbf{w}) = \beta_k^{(j)} \dots \beta_1^{(j)}$ ($j = 1, 2, \dots, n$). For \mathbf{w} running over all m -tuples of k -letter words, $k = 1, 2, \dots$ we consider the set $E(\mathfrak{A})$ of all points $(0.\mathbf{w}; 0.\mathbf{a}(\mathbf{w})) \in \mathbb{R}^{m+n}$; here $0.\mathbf{u}$ stands for $(0.u_1; \dots; 0.u_\ell)$ where u_1, \dots, u_ℓ are k -letter words. Then we define $\mathbf{P}(\mathfrak{A})$ as a closure in \mathbb{R}^{m+n} of the set $E(\mathfrak{A})$. Following the lines of Note 2.18 it can be shown that $\mathbf{P}(\mathfrak{A}) = \mathbf{P}(F_{\mathfrak{A}})$. We stress that \mathfrak{A} is a synchronous letter-to-letter transducer; that is why in the definition of the plot all m input words as well as corresponding n output words of the automaton must have pairwise equal lengths.

Given a real function $G: D \rightarrow \mathbb{R}^n$ with the domain $D \subset \mathbb{R}^m$, by the *graph of the function* (on the torus \mathbb{T}^{m+n}) we mean the point subset $\mathbf{G}_D(g) = \{(\mathbf{x} \bmod 1; G(\mathbf{x}) \bmod 1) : \mathbf{x} \in D\} \subset \mathbb{T}^{m+n}$. Note that if $\mathbf{y} = (y_1; \dots; y_k) \in \mathbb{R}^k$ then $\mathbf{y} \bmod 1$ stands for $(y_1 \bmod 1; \dots; y_k \bmod 1)$.

Theorem 5.5. *Let \mathfrak{A} be a finite automaton over the alphabet $\{0, 1, \dots, p-1\}$, let \mathfrak{A} have m inputs and n outputs, and let $G = (G_1; \dots; G_n): [\mathbf{a}, \mathbf{b}] = [a_1, b_1] \times \dots \times [a_m, b_m] \rightarrow [0, 1]^n$ (where $[a_i, b_i] \subset [0, 1]$, $G_i: [\mathbf{a}, \mathbf{b}] \rightarrow [0, 1]$, $i = 1, 2, \dots, m$) be a two times differentiable function such that all its second partial derivatives are continuous on $[\mathbf{a}, \mathbf{b}]$. If $\mathbf{G}(G) \subset \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^{m+n}$ then there exist an $m \times n$ matrix $\mathbf{A} = (A_{ij})$ and a vector $\mathbf{B} = (B_1; \dots; B_n)$ such that $A_{ij} \in \mathbb{Q} \cap \mathbb{Z}_p$, $B_j \in \mathbb{Q} \cap \mathbb{Z}_p \cap [0, 1]$ ($i = 1, 2, \dots, m$; $j = 1, 2, \dots, n$) and $G(\mathbf{x}) = (\mathbf{x}\mathbf{A} + \mathbf{B}) \bmod 1$ for all $\mathbf{x} \in [\mathbf{a}, \mathbf{b}]$. There are not more than a finitely many \mathbf{A} and \mathbf{B} such that $A_{ij} \in \mathbb{Q} \cap \mathbb{Z}_p$, $B_j \in \mathbb{Q} \cap \mathbb{Z}_p \cap [0, 1]$ ($i = 1, 2, \dots, m$; $j = 1, 2, \dots, n$) and $\mathbf{G}_{[\mathbf{a}, \mathbf{b}]}((\mathbf{x}\mathbf{A} + \mathbf{B}) \bmod 1) \subset \mathbf{P}(\mathfrak{A})$ for some $[\mathbf{a}, \mathbf{b}] \subset [0, 1]^m$; moreover, if $\mathbf{G}_{[\mathbf{a}, \mathbf{b}]}(\mathbf{x}\mathbf{A} + \mathbf{B}) \subset \mathbf{P}(\mathfrak{A})$ for some $[\mathbf{a}, \mathbf{b}] \subset [0, 1]^m$ then $\mathbf{G}_{\mathbb{R}^m}((\mathbf{x}\mathbf{A} + \mathbf{B}) \bmod 1) \subset \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^{n+m}$.*

Proof of Theorem 5.5. Let $F_{\mathfrak{A}} = (F_1; \dots; F_n): \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p^n$ be automaton function of the automaton \mathfrak{A} . Having $i \in \{1, 2, \dots, m\}$ and $j \in \{1, 2, \dots, n\}$ fixed, take arbitrary numbers $z_k \in \mathbb{Z}_p \cap \mathbb{Q} \cap [a_k, b_k]$, $k = 1, 2, \dots, i-1, i+1, \dots, m$, consider the map $\bar{F}_{ij}(z) = F_j(z_1; \dots; z_{i-1}; z; z_{i+1}; \dots; z_m)$ and the function $\bar{G}_{ij}(x) = G(z_1; \dots; z_{i-1}; x; z_{i+1}; \dots; z_m)$.

As $z_k \in \mathbb{Z}_p \cap \mathbb{Q} \cap [a_k, b_k]$ and $[a_k, b_k] \subset [0, 1]$ then the map $\bar{F}_{ij}: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is a finite automaton function: Actually the corresponding automaton \mathfrak{A}_{ij} is a sequential composition of the automaton \mathfrak{A} with autonomous automata \mathfrak{B}_k which produce accordingly purely periodic output words $\text{wrd}(z_k) \in \mathcal{W}^\infty$ (cf. Corollary 2.7) and feed accordingly k -th inputs ($k = 1, \dots, i-1, i+1, \dots, m$) of the automaton \mathfrak{A} while the output of the automaton \mathfrak{A}_{ij} is the j -th output of the automaton \mathfrak{A} .

Claim: We assert that $\mathbf{G}_{[a_i, b_i]}(\bar{G}_{ij}) \subset \mathbf{P}(\mathfrak{A}_{ij})$.

To prove the claim, firstly note that by Corollary 2.7, for every $k = 1, \dots, i-1, i+1, \dots, m$ we have that $z_k = 0.(\zeta_{T_k-1}^{(k)} \zeta_{T_k-2}^{(k)} \dots \zeta_0^{(k)})^\infty$ where T_k is a period length of z_k (see Subsection 2.2). Let T be the least common multiple of all t_i ; then $z_k = 0.(\eta_{T-1}^{(k)} \eta_{T-2}^{(k)} \dots \eta_0^{(k)})^\infty$ for all $k = 1, \dots, i-1, i+1, \dots, m$. Denote the right-infinite purely periodic word $\eta_{T-1}^{(k)} \eta_{T-2}^{(k)} \dots \eta_0^{(k)}^\infty$ via $u(z_k) = \tau_1^{(k)} \tau_2^{(k)} \dots$ for suitable $\tau_q^{(\ell)} \in \mathbb{F}_p$.

Take arbitrary $x \in [a_i, b_i]$ and put $\mathbf{x} = (z_1; \dots; z_{i-1}; x; z_{i+1}; \dots; z_m) \in [\mathbf{a}, \mathbf{b}]$; then $(\mathbf{x}; G(\mathbf{x})) \in \mathbf{P}(\mathfrak{A})$. Let $x = 0.\chi_1 \chi_2 \dots$ be a base- p expansion of x (the word $u(x) = \chi_1 \chi_2 \dots$ is right-infinite); then from the definition of the plot it follows that there exists a strictly increasing sequence $\bar{r}_1 < \bar{r}_2 < \dots$ over \mathbb{N} such that

$$\lim_{\ell \rightarrow \infty} 0.\bar{\chi}_1 \bar{\chi}_2 \dots \bar{\chi}_{\bar{r}_\ell} = x; \quad (5.84)$$

$$\lim_{\ell \rightarrow \infty} 0.\bar{\tau}_1^{(k)} \bar{\tau}_2^{(k)} \dots \bar{\tau}_{\bar{r}_\ell}^{(k)} = z_k \quad (k = 1, \dots, i-1, i+1, \dots, m); \quad (5.85)$$

$$\lim_{\ell \rightarrow \infty} 0.\mathbf{a}(\mathbf{u}_{\bar{r}_\ell}(\bar{x})) = G(\mathbf{x}), \quad (5.86)$$

where

$$\begin{aligned} \mathbf{u}_{\bar{r}_\ell}(\bar{x}) &= (u_{\bar{r}_\ell}(\bar{z}_1); \dots; u_{\bar{r}_\ell}(\bar{z}_{i-1}); u_{\bar{r}_\ell}(\bar{x}); u_{\bar{r}_\ell}(\bar{z}_{i+1}); \dots; u_{\bar{r}_\ell}(\bar{z}_m)); \\ u_{\bar{r}_\ell}(\bar{z}_k) &= \bar{\tau}_1^{(k)} \bar{\tau}_2^{(k)} \dots \bar{\tau}_{\bar{r}_\ell}^{(k)} \quad (k = 1, \dots, i-1, i+1, \dots, m); \\ u_{\bar{r}_\ell}(\bar{x}) &= \bar{\chi}_1 \bar{\chi}_2 \dots \bar{\chi}_{\bar{r}_\ell}, \end{aligned}$$

see remarks which follow Definition 5.4 above. Moreover, since base- p of all z_k are unique, the arguing like in the first part of the proof of Proposition 4.6 we conclude that there exists a state s of the automaton \mathfrak{A} and a strictly increasing sequence $r_1 < r_2 < \dots$ over \mathbb{N} such that

$$\lim_{\ell \rightarrow \infty} 0.\chi_1 \chi_2 \dots \chi_{r_\ell} = x; \quad (5.87)$$

$$\lim_{\ell \rightarrow \infty} 0.\tau_1^{(k)} \tau_2^{(k)} \dots \tau_{r_\ell}^{(k)} = z_k \quad (k = 1, \dots, i-1, i+1, \dots, m); \quad (5.88)$$

$$\lim_{\ell \rightarrow \infty} 0.\mathbf{a}_s(\mathbf{u}_{r_\ell}(x)) = G(\mathbf{x}), \quad (5.89)$$

where \mathfrak{A}_s is the automaton which differs from \mathfrak{A} only maybe by the initial state (which is s rather than s_0). Now recall that $\tau_1^{(k)} \tau_2^{(k)} \dots = (\eta_{T-1}^{(k)} \eta_{T-2}^{(k)} \dots \eta_0^{(k)})^\infty$ for all $k = 1, \dots, i-1, i+1, \dots, m$; so given $\ell \in \mathbb{N}$ let $q(\ell) \in \mathbb{N}$ be the largest such that $q_\ell < r_\ell$ and $\tau_{q_\ell}^{(k)} = \eta_0^{(k)}$ for some (thus, for all) $k = 1, \dots, i-1, i+1, \dots, m$. Since all the words $\tau_1^{(k)} \tau_2^{(k)} \dots$ are periodic with a period of length T such q_ℓ exists for all sufficiently large $\ell \geq N$. Denote via s_ℓ the state the automaton $\mathfrak{A}(s)$ reaches after being feeded (via respective inputs) by words $\tau_{q_\ell+1}^{(k)} \dots \tau_{r_\ell}^{(k)}$ ($k = 1, \dots, i-1, i+1, \dots, m$) and $\chi_{q_\ell+1} \dots \chi_{r_\ell}$. By the finiteness of the automaton, in the sequence $(s_\ell)_{\ell=N}^\infty$ at least one state, say \hat{s} , occurs infinitely many times; therefore from (5.87)–(5.89) it follows that

$$\lim_{\ell \rightarrow \infty} 0.\chi_1 \chi_2 \dots \chi_{q_\ell} = x; \quad (5.90)$$

$$\lim_{\ell \rightarrow \infty} 0.(\eta_{T-1}^{(k)} \eta_{T-2}^{(k)} \dots \eta_0^{(k)})^{q_\ell/T} = z_k \quad (k = 1, \dots, i-1, i+1, \dots, m); \quad (5.91)$$

$$\lim_{\ell \rightarrow \infty} 0.\mathbf{a}_{\hat{s}}(\mathbf{u}_{q_\ell}(x)) = G(\mathbf{x}), \quad (5.92)$$

where $\mathfrak{A}_{\hat{s}}$ is the automaton which differs from \mathfrak{A} only maybe by the initial state (which is \hat{s} rather than s_0). Note that T is a divisor of q_ℓ by the construction of

q_ℓ since all the words $\tau_1^{(k)}\tau_2^{(k)}\dots$ are periodic with a period of length T . By the definition of the plot we conclude that (5.90)–(5.92) prove our claim.

Thus the function \bar{G}_{ij} satisfies all conditions of Theorem 5.1; therefore the second derivative of \bar{G}_{ij} is zero. But this means by the construction of G_{ij} that every second partial derivative $\partial^2 G_j / \partial^2 x_i$ is zero for all $z_k \in \mathbb{Z}_p \cap \mathbb{Q} \cap [a_k, b_k]$ ($k = 1, \dots, i-1, i+1, \dots, m$) and all $x \in [a_i, b_i]$. As $\mathbb{Z}_p \cap \mathbb{Q} \cap [a_k, b_k]$ is dense in $[a_k, b_k]$ for all $k = 1, \dots, i-1, i+1, \dots, m$ we conclude that $\partial^2 G_j / \partial x_i^2 = 0$ everywhere on $[\mathbf{a}, \mathbf{b}]$ and for all $j = 1, 2, \dots, n$, $i = 1, 2, \dots, m$.

Now we are going to prove that $\partial^2 G_j / \partial x_i \partial x_t$ vanishes everywhere on $[\mathbf{a}, \mathbf{b}]$ and for all $j = 1, 2, \dots, n$, $i, t = 1, 2, \dots, m$, $i \neq t$ (without loss of generality, let $t > i$ in what follows). Assume that the opposite is true, that is, that there exist i, j, t and a point $\mathbf{x} \in [\mathbf{a}, \mathbf{b}]$ such that $\partial^2 G_j(\mathbf{x}) / \partial x_i \partial x_t \neq 0$. Then due to the continuity of second partial derivatives of the function G , by using the argument similar to that from the beginning of the proof of Lemma 5.3 we conclude that there exist a point (which without risk of misunderstanding we denote by the same symbol \mathbf{x}) in $(\mathbf{a}, \mathbf{b}) = (a_1, b_1) \times \dots \times (a_m, b_m)$ and a neighborhood U of that point such that $\partial^2 G_j / \partial x_i \partial x_t > 0$ everywhere on U . Therefore we always may take $z_k \in \mathbb{Z}_p \cap \mathbb{Q} \cap [a_k, b_k]$; $k \neq i, t$; $M \in \mathbb{N}$ and $c, d \in \{0, 1, \dots, p^M - 1\}$ such that the point $\mathbf{z}(x, y) = (z_1; \dots; z_{i-1}; x; z_{i+1}; \dots; z_{t-1}; y; z_{t+1}; \dots; z_m)$ lies in U for all $x = p^{-M}(c + e)$, $y = p^{-M}(d + h)$ and all $e, h \in [0, 1)$. Arguing like in the proof of Proposition 4.14 we see that the following inclusion holds:

$$\{(\bar{\mathbf{z}}(e, h); (p^M G(\bar{\mathbf{z}}(e, h))) \bmod 1) : e, h \in [0, 1]\} \subset \mathbf{P}(\mathfrak{A}),$$

where $\bar{\mathbf{z}}(e, h) = (\mathbf{z}(x, y)) \bmod 1$ (we reduce all coordinates modulo 1).

Consider a finite automaton $\tilde{\mathfrak{A}}$ which is obtained by ‘gluing together’ the i -th and the t -th inputs of the automaton \mathfrak{A} while feeding the rest k -th inputs with infinite words $\text{wr}d((p^M z_k) \bmod 1)$; that is, the automaton function of the automaton $\tilde{\mathfrak{A}}$ is

$$f_{\tilde{\mathfrak{A}}}(v) = f_{\mathfrak{A}}(w_1; \dots; w_{i-1}; v; w_{i+1}; \dots; w_{t-1}; v; w_{t+1}; \dots; w_m)$$

where $w_\ell = \text{wr}d((p^M z_k) \bmod 1) \in \mathcal{W}^\infty$, $\ell \in \{1, 2, \dots, m\} \setminus \{i, t\}$. By argument similar to that for the case $i = t$ (see the proof of the Claim above) we conclude that the automaton $\tilde{\mathfrak{A}}$ is finite and that the graph of the function $\bar{G}_j(h, h) = (p^M G_j(\mathbf{z}(p^{-M}(c+h), p^{-M}(d+h))) \bmod 1 : [0, 1]^2 \rightarrow [0, 1)$ when h is running through $[0, 1)$ lies in $\mathbf{P}(\tilde{\mathfrak{A}})$. But on the other hand we have that

$$\partial^2 \bar{G}_j(h, h) / \partial h^2 = (\partial / \partial x_i + \partial / \partial x_t)^2 G_j(\mathbf{z}(x, y)) = 2 \cdot \partial^2 G_j(\mathbf{z}(x, y)) / \partial x_i \partial x_t$$

since $\partial^2 G_j(\mathbf{z}(x, y)) / \partial x_i^2 = \partial^2 G_j(\mathbf{z}(x, y)) / \partial x_t^2 = 0$ by what we have already proved above. But this is a contradiction to Theorem 5.1 since the function $\bar{G}_j(h, h)$ of argument h satisfies all conditions of the theorem and has a non-zero second derivative. Thus we have proved that under conditions of Theorem 5.5 the function G must be affine: $G(\mathbf{x}) = \mathbf{x}\mathbf{A} + \mathbf{B}$ for all $\mathbf{x} \in [\mathbf{a}, \mathbf{b}]$.

Now fix arbitrary $i \in \{1, 2, \dots, m\}$, $j \in \{1, 2, \dots, n\}$, and $z_k \in [a_k, b_k] \cap \mathbb{Z}_p \cap \mathbb{Q}$ for $k = 1, 2, \dots, m$, $k \neq i$; consider the function \bar{G}_{ij} and the automaton $\tilde{\mathfrak{A}}_{ij}$ as in the beginning of the proof of Theorem 5.5. Then from the affinity of the function G it follows that $\bar{G}_{ij}(x) = xA_{ij} + B_j$. Since $\mathbf{G}_{[a_i, b_i]}(\bar{G}_{ij}) \subset \mathbf{P}(\tilde{\mathfrak{A}}_{ij})$ by the Claim above, Theorem 5.1 implies that $A_{ij}, B_j \in \mathbb{Z}_p \cap \mathbb{Q}$.

Further, arguing like in the proof of Proposition 4.14 we conclude that for suitable $M \in \mathbb{N}$ and $\mathbf{h} \in \{0, 1, \dots, p^M - 1\}^m$ the graph $\mathbf{G}_{[0, 1]^m}(H(\mathbf{v}))$ of the function $H(\mathbf{v}) = H_{\mathbf{h}, M}(\mathbf{v}) = (p^M((p^{-M}(\mathbf{h} + \mathbf{v})\mathbf{A} + \mathbf{B}) \bmod 1 = (\mathbf{v}\mathbf{A} + (\mathbf{h}\mathbf{A} + p^M\mathbf{B})) \bmod 1$ lies completely in $\mathbf{P}(\mathfrak{A})$. Now considering the function H and the corresponding automaton $\tilde{\mathfrak{A}}_{ij}$ as above for $z_k = 0$, $k = 1, 2, \dots, m$, $k \neq i$, $G = H$, we conclude by Theorem 5.1 that there are only finitely many A_{ij} ; whence finitely many \mathbf{A} .

If for some of these \mathbf{A} there were infinitely many $\mathbf{B} \bmod 1$ such that $\mathbf{G}_{[0,1]^m}(H(\mathbf{v})) \subset \mathbf{P}(\mathfrak{A})$ then for some $j \in \{1, 2, \dots, n\}$ there were infinitely many pairwise distinct $B_j \bmod 1$. But given arbitrary $z_k \in [a_k, b_k] \cap \mathbb{Z}_p \cap \mathbb{Q}$ for $k = 2, 3, \dots, m$ and considering corresponding automata $\bar{\mathfrak{A}}_{1j}$ for various $(m-1)$ -tuples (z_2, \dots, z_m) (cf. the beginning of the proof of Theorem 5.5), from the construction of $\bar{\mathfrak{A}}_{1j}$ it follows (cf. the proof of the Claim) that there are only finitely many these automata $\bar{\mathfrak{A}}_{1j}$ since the automaton \mathfrak{A} is finite. Therefore applying Theorem 5.1 to every automaton $\bar{\mathfrak{A}}_{1j}$ we finally conclude that there are only finitely many $B_j \bmod 1$; a contradiction to our assumption.

Therefore there are only finitely many pairwise distinct functions $H_{\mathbf{h}, M}$ as above. Now by mimic the respective part of the proof of the first assertion of Theorem 5.1 we conclude that given an $(m \times n)$ -matrix \mathbf{A} and a vector \mathbf{B}_j over $\mathbb{Z}_p \cap \mathbb{Q}$ such that the graph of the function $G(\mathbf{x}) = \mathbf{x}\mathbf{A} + \mathbf{B}$ on $[\mathbf{a}, \mathbf{b}] \subset [0, 1]^m$ lies completely in $\mathbf{P}(\mathfrak{A})$ then necessarily $\mathbf{G}_{\mathbb{R}^m}((\mathbf{x}\mathbf{A} + \mathbf{B}) \bmod 1) \subset \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^{n+m}$. \square

Note 5.6. An automaton with a single input and a single output over respective alphabets $\{0, 1, \dots, p^n - 1\}$ and $\{0, 1, \dots, p^k - 1\}$, $(n, k \geq 1)$, can be considered as an automaton with n inputs and k outputs over an alphabet $\{0, 1, \dots, p - 1\}$ and therefore Theorem 5.5 can be applied to automata of that sort as well.

6. DISCUSSION: *It from bit*, INDEED

Now we are going to outline possible relations of main results of preceding section to quantum theory leaving apart applications to cryptography (the latter are subject of future paper). Although further physical interpretation of the results is highly speculative, it reveals deep analogies between automata and quantum systems and thus worth a short discussion to explain a direction in which it is reasonable to develop the results in order to derive some physically meaningful assertions (and maybe models) from mathematical theorems of the paper.

We start with some remarks on what is ‘physical law’. Let us (somewhat naively) think of a physical law as of mathematical correspondence between quantities which express impacts a physical system is exposed to and quantities which express responses the system exhibits. Suppose for simplicity that both impacts and responses are scalars. As the measured experimental values of physical quantities are rational numbers (since there is no possibility to obtain during measurements an exact value of irrational number, cf. [42, 24, 25]) the result of measurements are points in \mathbb{R}^2 , the experimental points. To find a particular physical law one seeks for a correspondence between cluster points (w.r.t. the metrics in \mathbb{R}) of experimental values and tries to draw an experimental curve. The latter curve is a (piecewise) smooth curve (the C^2 -smoothness is common) which is the best approximation of the set of the experimental points. A physical law is then a curve which approximate with the highest achievable accuracy (w.r.t. metric in \mathbb{R}^2) the experimental curves obtained during series of measurements.

Let physical quantities which correspond to impacts and reactions be quantized; i.e. let they take only values (measured in suitable units and properly normalized), say, $0, 1, \dots, p - 1$, where $p > 1$ is an integer. Then, once the system is exposed to a sequence of k of impacts, it produces corresponding sequence of k reactions. Every impact changes current state of the system to a new one; therefore provided the systems is causal, both the next state and the reaction (effect) depends only on impacts (causes) the system has already been exposed to; so an automaton \mathfrak{A} is an adequate

model of the system¹. Every finite sequence $\alpha_{k-1}, \dots, \alpha_0$ of impacts/reactions corresponds to a base- p expansion of natural number $z = \alpha_{k-1}p^{k-1} + \dots + \alpha_0$ to which after normalization there corresponds a rational number $\frac{z}{p^k}$. Every measurement is a sequence of interactions $\alpha_{k-1}, \dots, \alpha_0$ of the measurement instrument with the system, and if the accuracy of the instrument is not better than p^{-N} , then the result of a single measurement lies within the segment $[\frac{z}{p^k} - p^{-N}, \frac{z}{p^k} + p^{-N}]$. Assuming that $k \gg N$ we see that even if the system before every measurement has been prepared in a fixed state s_0 (the initial state of the automaton) during a single measurement the system $\mathfrak{A}(s_0)$ will be exposed to a random sequences of impacts $\alpha_{k-M-1}, \dots, \alpha_0$ which switches the system to a new state $s = s(\alpha_{k-1}, \dots, \alpha_0)$; so actually as a result of the measurement due to its limited accuracy we obtain an experimental point $(0.\alpha_k \dots \alpha_{k-M}; 0.\beta_k \dots \beta_{k-M}) \in \mathbb{R}^2$ where $\beta_k \dots \beta_{k-M}$ is the output of the automaton $\mathfrak{A}(s)$ (whose initial state is $s = s(\alpha_{k-1}, \dots, \alpha_0)$) fed by the sequence $\alpha_k, \dots, \alpha_{k-M}$.

Theorem 5.1 shows that if the number of states of the system \mathfrak{A} is much less than the length of input sequence of impacts then experimental curves necessarily tend to straight lines (or torus windings, under a natural map of the unit square onto a torus), cf. Figures 1, 2, and 3. This may be judged as linearity of corresponding physical law and, what is even more important, the way experimental points are clustering on the unit square is very much alike to that of the points where electrons hit target screen in a double-slit experiment, cf. Figures 1–2 and Figure 14. We are not going here to discuss further parallels of the computer experiments with automata and behaviour of quantum systems such as analogies between transition and ergodic states of automata and mixed and pure quantum states respectively, or probabilities of Markov chain related to an automaton and probabilities in quantum systems, etc.: Although we believe that the analogies are not external but reflect deep relations between quantum systems and automata, the issues are far from the subject of the paper and that's why the discussion is postponed to further relevant papers. Here we briefly touch only an interesting analogy between smooth curves in plots of finite automata and matter waves of quantum theory.

By Theorem 5.1, the smooth curves from the plot of a finite automaton \mathfrak{A} can be described by families of complex-valued exponential functions of the form $\psi_k(y) = e^{i(Ay - 2\pi p^k B)}$, $k = 0, 1, 2, \dots$, for suitable $A, B \in \mathbb{Z}_p \cap \mathbb{Q}$, cf. Corollary 3.13. The wave function of a particle is of the form $ce^{i(mx - t\omega)}$ where m is momentum, x position, ω angular frequency, and c is a complex amplitude. Comparing the two expressions we see that p^k may serve as a time for the automaton \mathfrak{A} since multiplication by p^k is a k -step shift of a base- p expansion of a number. But can we somehow associate it to physical time t of quantum theory? In what follows we argue that yes, there is a natural way to do this.

Let us forget for a moment that p is a positive integer and suppose that $p = 1 + \tau$ where $1 \gg \tau > 0$ is a small real number; then $p^k \approx 1 + k\tau$ and if τ is a small time interval which is out of accuracy of measurements (e.g., let τ be Planck time which is approximately 10^{-43} s.). Therefore the torus link $\psi_k(y) = e^{i(Ay - 2\pi p^k B)}$, $k = 0, 1, 2, \dots$ can be approximately described by $\Psi(y, t) = e^{-i \cdot 2\pi B} e^{i(Ay - 2\pi t B)}$, $y, t \in \mathbb{R}$ since it is reasonable to assume that $k\tau$ is just a time t as τ is a small time interval, a time quantum, the Planck time. But $\Psi(y, t)$ is a wave function of

¹We stress that we are *not* speaking here about the so-called memory effect of the macroscopic measurement equipment which may ‘remember’ its previous interactions with particles, cf. [13]; we only say that every interaction (impact) forces the system (e.g. a particle) to change its state to some another one. We do *not* discuss the nature of these states which are *not* necessarily quantum states; we just say that every interaction changes something in a system and refer to this ‘something’ as to a ‘state’ of the system, and nothing more.

FIGURE 14. Interference pattern of the double slit experiment. From Wikimedia Commons, the free media repository http://commons.wikimedia.org/wiki/File:Double-slit_experiment_results_Tanamura_four.jpg

a particle with momentum A , angular frequency $2\pi B$ and amplitude $e^{-i \cdot 2\pi B}$. Is this mathematically correct to substitute $1 + \tau$ for p in our reasoning? Yes, this is correct; but to explain why this is correct we need to recall a notion of β -*expansion* of real number.

The β -expansions are radix expansions in non-integer bases; they were first introduced more than half-century ago, see [37, 35], and now β -expansions are a substantial part of dynamics, see e.g. survey [40]. Following [40], given $x \in [0, 1]$ and $\beta \in \mathbb{R}$, $\beta > 1$ we call a sequence $(\chi_i)_{i=1}^{\infty}$ over the alphabet $\{0, 1, \dots, \lfloor \beta \rfloor\}$ a β -*expansion* of x once $x = \sum_{i=1}^{\infty} \chi_i \beta^{-i}$ for suitable $N \in \mathbb{Z}$. Note that sometimes the term β -expansion is used in a narrower meaning, when the ‘digits’ χ_i are obtained by the so-called ‘greedy algorithm’ only, cf. [29, Section 7.2] but this is not important at the moment: In what follows we just sketch the way how the results of current paper can be modified to handle the case of β -expansions rather than the case of base- p expansions only. We leave details and rigorous proofs for further paper.

From the definition we see that the notion of β -expansion is a generalization of the notion of base- p expansion: It is clear that for $\beta = p$ the β -expansion of x is just base- p expansion of x , and that is why both β -expansions and base- p expansions share some common properties. For instance, given β -expansion of reals it is possible to perform arithmetic operations with reals in a way similar to that of school-textbook algorithms for base- p expansions of reals. However, differences

between base- p expansions and β -expansions should also be taken into the account since when β is not an integer, a β -expansion of a real number is generally not unique; moreover a real number may have a continuum of different β -expansions for β fixed. Nonetheless, we can perform arithmetic operations with numbers represented by β -expansions, i.e., with words over the alphabet $\{0, 1, \dots, \lfloor \beta \rfloor\}$. These operations for some non-integer β may be represented by finite automata as well. For instance, if $\beta = \sqrt[3]{2}$ then arithmetic operations with numbers represented by $\sqrt[3]{2}$ -expansions $\dots \alpha_2 \alpha_1 \alpha_0$ and $\dots \gamma_2 \gamma_1 \gamma_0$ (which are binary words over the alphabet $\{0, 1\}$ since $\lfloor \sqrt[3]{2} \rfloor = 1$) can be performed in a manner similar to that when one applies school-textbook algorithms for base- p expansions, with the only difference: A ‘carry’ from i -th position should be added to $(n+i+1)$ -th position; e.g. for $\beta = \sqrt{2}$ we have that $11 + 01 = 110$ while in the case $\beta = 2$ we have that $11 + 01 = 100$. Note that $01 = 1$, $11 = \sqrt{2} + 1$ (and thus $110 = (\sqrt{2})^2 + (\sqrt{2})^1 + 0 = 2 + \sqrt{2}$) when $\beta = \sqrt{2}$; and $01 = 1$, $11 = 3$ when $\beta = 2$.

When an automaton \mathfrak{A} proceeds a word (or, a corresponding system reacts to impacts) it just evaluates step-by-step a p -adic 1-Lipschitz function $f_{\mathfrak{A}}: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ (cf. Subsection 2.4), and no β appears at this moment. But we need to specify β when we ‘visualize’ the function $f_{\mathfrak{A}}$ in \mathbb{R}^2 : To every word $\alpha_{k-1} \dots \alpha_0$ over the alphabet $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ we put into the correspondence a point $(\beta^{-k}(\alpha_{k-1}\beta^{k-1} + \dots + \alpha_1\beta + \alpha_0)) \bmod 1 \in [0, 1)$; thus to every pair of input/output words of the automaton there corresponds a point in the unit square \mathbb{T}^2 (or, on the unit torus $\mathbb{T}^2 \subset \mathbb{R}^3$). We then take a closure of all these points and obtain a β -plot of the automaton \mathfrak{A} in a way similar to that when we constructed a plot of the automaton (which corresponds to the case when $\beta = p$), cf. Definition 2.16. We then consider smooth curves in the β -plots of finite automata, in particular, the curves which correspond to affine automata functions $z \mapsto Az + B$. To these functions there correspond torus windings which can be expressed in a form of complex-valued functions $\psi_k(y) = e^{i(Ay - 2\pi\beta^k B)}$, $k = 0, 1, 2, \dots$, $y \in \mathbb{R}$; and these functions can be approximated with arbitrarily high accuracy by functions $\Psi(y, t) = e^{-i \cdot 2\pi B} e^{i(Ay - 2\pi t B)}$, $t, y \in \mathbb{R}$, just by taking $\beta > 1$ sufficiently close to 1. Moreover, the case when β is close to 1 is the only case when approximations are of the form of wave functions. But this means that the *corresponding automata must necessarily be binary*; i.e., their input/output alphabets are $\{0, 1, \dots, \lfloor \beta \rfloor\} = \{0, 1\}$. So these automata (which are just models of causal discrete systems) indeed produce waves, the *its*, from bits.

From this view, main results of the current paper may be considered as a contribution to informational interpretation of quantum theory, namely, to J. A. Wheeler’s *It from bit* doctrine which suggests that all things physical (‘its’) are information-theoretic in origin (‘from bits’), [46]: We have given some evidence above that this is indeed so regarding particular ‘its’, the matter waves. We stress once again that our conclusion is based on the following assumptions only: A quantum system is causal and discrete, whence is an automaton; and the number of states of the automaton is finite.

REFERENCES

- [1] Charalambos D. Aliprantis and Owen Burkinshaw. *Principles of real analysis*. Academic Press, Inc., third edition, 1998.
- [2] J.-P. Allouche and J. Shallit. *Automatic Sequences. Theory, Applications, Generalizations*. Cambridge Univ. Press, 2003.
- [3] V. Anashin and A. Khrennikov. *Applied Algebraic Dynamics*, volume 49 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter GmbH & Co., Berlin—N.Y., 2009.
- [4] V. S. Anashin, A. Yu. Khrennikov, and E. I. Yurova. Characterization of ergodicity of p -adic dynamical systems by using van der Put basis. *Doklady Mathematics*, 83(3):306–308, 2011.

- [5] Vladimir Anashin. Automata finiteness criterion in terms of van der Put series of automata functions. *p-Adic Numbers, Ultrametric Analysis and Applications*, 4(2):151–160, 2012.
- [6] Vladimir Anashin. The non-Archimedean theory of discrete systems. *Math. Comp. Sci.*, 6(4):375–393, 2012.
- [7] Andre Barbé and Friedrich von Haeseler. Limit sets of automatic sequences. *Adv. Math.*, 175:169–196, 2003.
- [8] W. Brauer. *Automatentheorie*. B. G. Teubner, Stuttgart, 1984.
- [9] John Carroll and Darrell Long. *Theory of Finite Automata*. Prentice-Hall Inc., 1989.
- [10] A. N. Cherepov. On approximation of continuous functions by determinate functions with delay. *Discrete Math. Appl.*, 22(1):1–24, 2010.
- [11] A. N. Cherepov. Approximation of continuous functions by finite automata. *Discrete Math. Appl.*, 22(4):445–453, 2012.
- [12] R. Crowell and R. Fox. *Introduction to the Knot Theory*. Ginn and Co., Boston, 1963.
- [13] D. Dubischar, V. M. Gundlach, O. Steinkamp, and A. Khrennikov. The interference phenomenon, memory effects in the equipment and random dynamical systems over the fields of p -adic numbers. *Nuovo Cimento B*, 114(4):373–382, 1999.
- [14] B. A. Dubrovin, A. T. Fomenko, and S. P. Novikov. *Modern Geometry - Methods and Applications*, volume II. Springer-Verlag, NY–Berlin–Heidelberg–Tokyo, 1985.
- [15] Samuel Eilenberg. *Automata, Languages, and Machines*, volume A. Academic Press, 1974.
- [16] C. Frougny and K. Klouda. Rational base number systems for p -adic numbers. *RAIPO Theor. Inform. Appl.*, 46(1):87–106, 2012.
- [17] F. Q. Gouvêa. *p-adic Numbers, An Introduction*. Springer-Verlag, Berlin–Heidelberg–New York, second edition, 1997.
- [18] R. I. Grigorichuk, V. V. Nekrashevich, and V. I. Sushchanskii. Automata, dynamical systems, and groups. *Proc. Steklov Institute Math.*, 231:128–203, 2000.
- [19] B. Hasselblatt and A. Katok. *A First Course in Dynamics*. Cambridge Univ. Press, Cambridge, etc., 2003.
- [20] S. Katok. *p-adic analysis in comparison with real*. Mass. Selecta. American Mathematical Society, 2003.
- [21] John G. Kemeny and J. Laurie Snell. *Finite Markov Chains*. Springer-Verlag, 1976.
- [22] A. Khrennikov. Quantum mechanics from time scaling and random fluctuations at the “quick time scale”. *Nuovo Cimento B*, 121(9):1005–1021, 2006.
- [23] A. Khrennikov. To quantum averages through asymptotic expansion of classical averages on infinite-dimensional space. *Math. Phys.*, 48(1), 2007. Art. No. 013512.
- [24] A. Yu. Khrennikov. Ultrametric Hilbert space representation of quantum mechanics with a finite exactness. *Found. Physics*, 26:1033–1054, 1996.
- [25] A. Yu. Khrennikov. *Non-Archimedean Analysis: Quantum Paradoxes, Dynamical Systems and Biological Models*. Kluwer Academic Publishers, Dordrecht, 1997.
- [26] N. Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate texts in math*. Springer-Verlag, second edition, 1984.
- [27] Michal Konečný. Real functions computable by finite automata using affine representations. *Theor. Comput. Sci.*, 284:373–396, 2002.
- [28] L. P. Lisovik and O. Yu. Shkaravskaya. Real functions defined by transducers. *Cybernetics and System Analysis*, 34(1):69–76, 1998.
- [29] M. Lothaire. *Algebraic Combinatorics on Words*. Cambridge Univ. Press, 2002.
- [30] A. G. Lunts. The p -adic apparatus in the theory of finite automata. *Problemy Kibernetiki*, 14:17–30, 1965. In Russian.
- [31] K. Mahler. *p-adic numbers and their functions*. Cambridge Univ. Press, 1981. (2nd edition).
- [32] V. Mansurov. *Knot theory*. Chapman & Hall/CRC, Boca Raton - London - NY - Washington, 2004.
- [33] A. Mishchenko and A. Fomenko. *A course of differential geometry and topology*. Mir, Moscow, 1988.
- [34] A. F. Monna. Sur une transformation simple des nombres p -adiques en nombres réels. *Indag. Math.*, 14:1–9, 1952.
- [35] W. Parry. On the β -expansions of real numbers. *Acta Math. Acad. Sci. Hung.*, 11:401–416, 1960.
- [36] M. B. Pour-El and J. I. Richards. *Computability in Analysis and Physics*. Springer-Verlag, 1989.
- [37] A. Rényi. Representation for real numbers and their ergodic properties. *Acta Math. Acad. Sci. Hung.*, 8:477–493, 1957.
- [38] W. H. Schikhof. *Ultrametric calculus*. Cambridge University Press, 1984.
- [39] O. Yu. Shkaravskaya. Affine mappings defined by finite transducers. *Cybernetics and System Analysis*, 34(5):781–783, 1998.

- [40] N. Sidorov. Arithmetic dynamics. In S. Bezuglyi and S. Kolyada, editors, *Topics in dynamics and ergodic theory*, volume 310 of *London Math. Soc. Lecture Note Series*, pages 145–189. Cambridge University Press, Cambridge, 2003.
- [41] T. I. Smyshlyaeva. A criterion for functions defined by automata to be bounded-determinate. *Diskret. Mat.*, 25(2):121–134, 2013.
- [42] V. S. Vladimirov, I. V. Volovich, and E. I. Zelenov. *p-adic Analysis and Mathematical Physics*. World Scientific, Singapore, 1994.
- [43] J. Vuillemin. On circuits and numbers. *IEEE Trans. on Computers*, 43(8):868–879, 1994.
- [44] J. Vuillemin. Finite digital synchronous circuits are characterized by 2-algebraic truth tables. In *Advances in computing science - ASIAN 2000*, volume 1961 of *Lecture Notes in Computer Science*, pages 1–7, 2000.
- [45] J. Vuillemin. Digital algebra and circuits. In *Verification: Theory and Practice*, volume 2772 of *Lecture Notes in Computer Science*, pages 733–746, 2003.
- [46] John A. Wheeler. Information, physics, quantum: The search for links. In W. H. Zurek, editor, *Complexity, Entropy, and the Physics of Information*, pages 309–336, Redwood City, Calif., 1990. Addison-Wesley Pub. Co.
- [47] S. V. Yablonsky. *Introduction to discrete mathematics*. Mir, Moscow, 1989.

This figure "1024px-2slit.jpg" is available in "jpg" format from:

<http://arxiv.org/ps/1502.01920v1>

This figure "5knot-infty-16.jpg" is available in "jpg" format from:

<http://arxiv.org/ps/1502.01920v1>

This figure "5knot-infty-16.png" is available in "png" format from:

<http://arxiv.org/ps/1502.01920v1>

This figure "5knot-infty-Monna.png" is available in "png" format from:

<http://arxiv.org/ps/1502.01920v1>

This figure "5knot.png" is available in "png" format from:

<http://arxiv.org/ps/1502.01920v1>

This figure "5x-blur-overlay.jpg" is available in "jpg" format from:

<http://arxiv.org/ps/1502.01920v1>

This figure "5x-blur.png" is available in "png" format from:

<http://arxiv.org/ps/1502.01920v1>

This figure "Torus-2link-new.jpg" is available in "jpg" format from:

<http://arxiv.org/ps/1502.01920v1>

This figure "Torus-link3_5x+1_3-2.JPG" is available in "JPG" format from:

<http://arxiv.org/ps/1502.01920v1>

This figure "Cable5_3-7-new.jpg" is available in "jpg" format from:

<http://arxiv.org/ps/1502.01920v1>

This figure "Parallel.JPG" is available in "JPG" format from:

<http://arxiv.org/ps/1502.01920v1>